Décembre

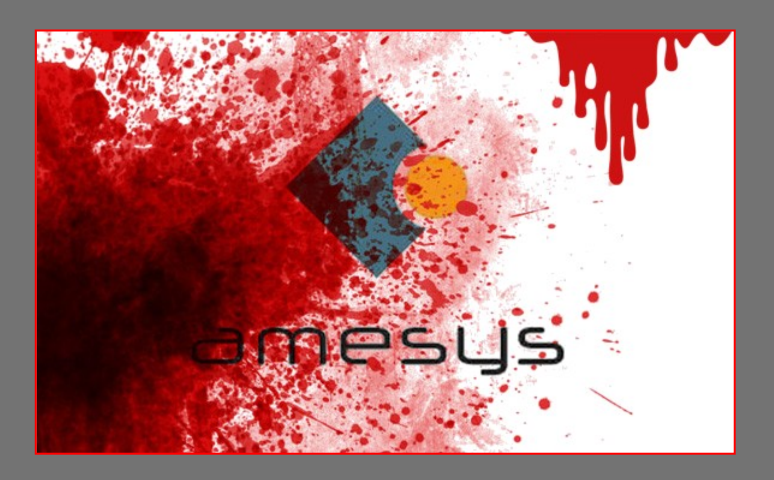
2011

Alerte : internet sous surveillance !

État des lieux, exportations et contrôle démocratique des outils de surveillance de l'Internet

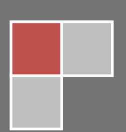
Le « *Deep Packet Inspection* », exportations d'un savoir-faire français

Table ronde du mercredi 14 décembre 2011 à l'Assemblée Nationale à l'initiative et invitation de monsieur le député Christian Paul.



Compte rendu textuel non officiel de l'enregistrement sonore agrémenté de liens référents et d'annexes pour comprendre des enjeux discutés.

Document finalisé le 31 décembre 2011.





Observations des rédacteurs

Cette transcription réalisée -initialement par Lpenet, Patchidem et Seb, puis corrigée, *sourcée* et mise en forme par des lecteurs de *Reflets.info* comme Mi0 et d'autre volontaires- à partir du document sonore n'est en rien officielle et ne peut se prévaloir comme telle. Réalisée par des amateurs, dans un outil de traitement de texte grand public, elle peut ne pas observer les règles typographiques en vigueur. Les propos des différents intervenants ont été dans la mesure du possible le plus fidèlement rapportés aux dépens parfois de règles syntaxiques et orthographiques afin de ne pas perdre la spontanéité des échanges et débats. Seules, quand la compréhension des propos l'exigeait, des formules ont été arrangées (syntaxe, ponctuation, répétitions) afin de ne pas perdre en clarté. Certains propos n'ont pu être attribués à un intervenant particulier, faute de savoir qui parlait lors des échanges ; ces derniers sont identifiés comme « intervenant non reconnu ». Enfin, des propos n'ont pas été reproduits faute d'avoir été compris, ils ont été mentionnés comme « commentaire inaudible ». Il est possible que des erreurs d'attribution de propos aient été insérées. Si vous êtes en mesure de reconnaitre des termes non compris ou d'attribuer une parole à un intervenant qui n'a pas été reconnu ou qui a été mal attribuée, prière de contacter la rédaction de Reflets.info afin de mettre le document à jour. Les échanges sont horodatés, de sorte de pouvoir retrouver dans le document sonore (cité en note de fin de page n°1, ou ci-dessous) les interventions souhaitées directement. Toutes les déclarations se référant à un évènement factuel, une révélation ou un article de presse ou blog en ligne, ont été agrémentées de notes de fin de page afin de consulter la référence à l'information donnée. Vous pouvez pour suivre les débats le plus fidèlement possible directement consulter le document sonore en ligne, non traité et non découpé.

Document sonore de cette table ronde du 14 décembre 2011 disponible sur le lien suivant :
http://soundcloud.com/anontranslator/conf-rence-deep-packet

Ce document a été mis en forme et publié afin de conserver un témoignage de cette table ronde, de s'efforcer de la propager dans la sphère publique, et de servir de mini-référentiel suite à l'ajout de notes de suivi des évènements et déclarations Ce document est diffusé sous licence Creative Commons. Cela signifie que vous êtes libre de l'héberger, de le diffuser, de le dupliquer ou encore de le modifier.

SYNOPSIS

« Ce n'est plus un doute, la menace est avérée dans de nombreux pays. Des technologies de surveillance des réseaux, des communications, et des échanges numériques se développent et sont utilisées à l'insu des citoyens. Nos libertés numériques, indispensables à la démocratie du XXIème siècle, en sont la cible. Ainsi, la vente à la Libye de telles technologies par une entreprise française et après le feu vert du gouvernement de notre pays a rendu possible la surveillance des populations et de l'opposition à ce régime autoritaire. Cet exemple qui n'est pas isolé démontre l'urgence d'un contrôle strict de la production, de l'usage et de l'exportation de ces moyens de surveillance et de contrôle numériques. Des médias d'investigation témoignent, des questions au gouvernement restent sans réponses, une commission d'enquête parlementaire est demandée. Etat des lieux du « *paysage de la surveillance* », cas concrets d'atteintes aux libertés démocratiques, réactions citoyennes et législatives, seront les thèmes abordés. » **Christian Paul**.

M. Christian Paul, député. Et bien si vous voulez on va commencer cette table ronde[1], merci d'abord avoir répondu à mon invitation, d'être venu à l'assemblée nationale pour évoquer ce soir un certain nombre de problèmes qui sont à mes yeux, à nos yeux je pense aussi, de graves manquements aux valeurs démocratiques et qui concernent donc, la façon dont les technologies de surveillance des réseaux numériques sont aujourd'hui produites en France, exportées hors de France et singulièrement ces dernières années dans des pays qui étaient ou qui sont encore, je pense à la Syrie en particulier, des dictatures, et la manière aussi dont probablement ces technologies sont en train d'être disséminées de différentes façons dont on parlera également sur le territoire français.

Cette table ronde elle a deux trois motifs très simples, le premier c'est d'amplifier l'alerte qui a été lancée depuis plusieurs mois maintenant et notamment par quelques-uns de ceux qui sont autour de moi et que je vous présenterais dans quelques instants en tout cas par un certain nombre de médias, beaucoup de journalistes ont fait sur ces questions, qu'il s'agisse d'ailleurs de journalistes des médias purement Internet ou d'autres médias plus traditionnels, il y a un très gros travail qui a été fait ces derniers mois je veux le souligner d'emblée, donc amplifier cette alerte, partager nos informations aussi parce qu'on a affaire à un monde opaque, il est important que le résultat de ses investigations on puisse le mettre en commun bien sûr. Les menaces de surveillance générale et du Net sont aujourd'hui avérées, plus que des menaces d'ailleurs, la France a vendu ces technologies en Libye, c'est aujourd'hui non contesté, y compris par l'entreprise qui les a commercialisées, des informations inquiétantes également à propos de la Syrie nous sont parvenues, c'est une autre entreprise française, et nous évoquerons tout à l'heure également la Tunisie. Donc l'objectif c'est vraiment de faire un état des lieux de ce qui se passe aujourd'hui, d'exprimer également, en tout cas je souhaite le faire et je pense que vous partagerez largement, une demande de contrôle démocratique sur ces technologies, sur leurs conditions d'exportations peut-être même sur leurs exportations tout court.

Informé par certains d'entre vous j'avais posé au premier ministre une question écrite à la fin du mois d'août, depuis nous sommes une dizaine de parlementaires ici à avoir interrogé François Fillon sans obtenir jusqu'ici aucune réponse[2] sur la manière et les conditions dans lesquelles les technologies d'Amesys cette filiale de Bull ont été exportées, donc sont sorties de France, ont été vendues après 2007 au régime de Kadhafi. Nous continuerons évidemment à poser cette question, probablement d'ailleurs dans les prochaines semaines sous la forme de questions d'actualité. Nous avons demandé ici, le groupe socialiste a demandé ici une commission d'enquête parlementaire[3] pour avoir un outil d'investigation, puisque vous savez que devant ces commissions on parle sous serment, nous attendons donc avec impatience la venue des représentants du ministère de la défense et du premier ministre, et des entreprises concernées, devant une commission d'enquête parlementaire, cette commission d'enquête c'est bien sûr maintenant de la décision de la majorité du moment, à l'assemblée nationale dont elle dépend, pour l'instant on est dans la procédure. Il y a toujours moyen de faire durer quelques semaines de plus cette procédure, donc nous n'avons pas aujourd'hui de réponse ni positive ni négative de la part de la majorité UMP de l'assemblée nationale. Quand nous aurons cette réponse, si elle est positive nous aurons une commission d'enquête parlementaire, si elle ne l'est pas, nous attendons bien évidemment de nos collègues sénateurs qu'ils puissent à ce moment-là, prendre le relais. Ils sont évidemment sensibilisés, ils suivent avec leur président Jean-Pierre Bel très attentivement cette affaire et ces différents dossiers.

Mais je pense qu'il faudrait et je voulais le dire aussi ce soir, je pense qu'il faudrait aller plus loin bien sûr que de l'investigation, il faudrait des positions beaucoup plus fermes, et on peut les prendre très tôt, dans l'année 2012 et je crois que c'est vraiment un moratoire sur les exportations de ces technologies qu'il faudrait exiger dès maintenant, pourquoi pas d'ailleurs dès ce soir, afin de faire d'abord toute la lumière sur ce qui s'est passé,

---

1 Conférence Deep Packet Inspection à l'Assemblée Nationale : http://soundcloud.com/anontranslator/conf-rence-deep-packet

2 A la date de la table ronde, aucune réponse n'avait été formulée aux parlementaires (CF Annexe 1). Depuis, des réponses (non concluantes) ont été données (CF Annexe 2).

3 Proposition de résolution tendant à la création d'une commission d'enquête chargée de présenter les modalités concrètes de l'assistance prêtée par la France au régime du colonel Kadhafi en application des accords bilatéraux – notamment de l'accord de défense – entrés en vigueur à partir du mois de septembre 2007, et les conséquences pour les populations libyennes : http://www.assemblee-nationale.fr/13/propositions/pion3892.asp

et mettre un coup d'arrêt très ferme à la dissémination de ces technologies dans des conditions qui apparaissent aujourd'hui très mal contrôlées. Parce que, ou bien il s'agit de matériel, véritablement de guerre électronique, et dans ce cas-là il doit passer devant la commission interministérielle qui régit l'exportation des matériels de guerre, c'est là-dessus que j'avais d'ailleurs interrogé le premier ministre, sans réponse jusqu'ici, ou bien ce ne sont pas des matériels qui doivent passer actuellement au regard des règles en vigueur, devant cette commission, et, dans ce cas-là, il faut très probablement étendre la liste des équipements qui doivent obligatoirement passer devant la commission avant toute exportation, donc un moratoire c'est une façon de donner un coup d'arrêt à ces pratiques qui sont évidemment aujourd'hui, tout à fait scandaleuses, au regard des droits de l'homme évidemment, et de la façon dont la France doit se comporter à l'égard de pays qui subissent des régimes autoritaires.

D'ailleurs il est tout-à-fait intéressant de regarder à cet égard le rapport qui est fait au parlement sur les exportations d'armement en France en 2010[4], c'est un rapport qui est fait par le ministère de la défense, et on lit une phrase qui prend ici tout son sens, puisque sous la signature du ministre de la défense on lit : « *la France prend en compte les situations de conflit et les atteintes graves aux droits de l'homme, notre pays considère que toute fourniture de matériel susceptible de concourir à la répression interne des populations civiles doit être refusée* ». Bon, mon sentiment, vous me direz ce que vous en pensez, c'est qu'on est très clairement devant une situation de cet ordre là, et donc il y a double langage et un immense cynisme d'état dans cette affaire, et il y a aussi un immense cynisme commercial de la part de ceux qui vendent ces produits, je vous citerais simplement un extrait d'un propos qui est tenu par un ingénieur de l'entreprise Amesys que vous avez cité d'ailleurs dans un article[5] publié sur le site Owni cet après-midi. Interrogé sur le fait que ce type de pratique commerciale pouvait porter un coup en terme d'image à l'entreprise Amesys et même à l'entreprise Bull, l'ingénieur en question répond, et c'est extraordinaire, c'est pour ça que je voulais vous le relater : « *le grand public n'est jamais notre client* ». Voilà donc dans quel état d'esprit effectivement on procède aujourd'hui.

M. Jean-Marc Manach, journaliste. (7 min 39 s). Et juste après il précise : « *et le scandale nous a permis de toucher un nouveau prospect* ».

M. Christian Paul, député. (7 min 44 s). Oui c'est ça : « *par contre ça nous a déjà généré une touche commerciale pour un pays qu'on ne connaissait pas* ». Voilà comment aujourd'hui une entreprise française, avec forcément un feu vert politique, à quel moment, à quel niveau, dans le cadre des accords de coopération de sécurité qui ont été passé d'ailleurs en 2007 avec la Libye, voilà comment des entreprises françaises se signalent hors de nos frontières. Alors il y a tout ce qui se passe à l'extérieur, on va y revenir bien sûr avec nos invités, mais il y a aussi la nécessité de prévenir des utilisations arbitraires en France.

Là aussi il est toujours compliqué d'appréhender la réalité du risque, mais plusieurs d'entre vous ont signalé la façon dont aujourd'hui on déployait des sondes sur les réseaux numériques en France, pour quels usages, est-ce qu'il s'agit d'usages d'interception, qui ressemblent toute similitude gardée avec ce qui était jadis et encore aujourd'hui les écoutes téléphoniques, transposé au monde des réseaux numériques, pour quel usage, dans quelles conditions sous quel contrôle, de quoi s'agit-il ? Voilà des questions que nous souhaitons également poser. En tout cas l'encadrement de ces pratiques est évidemment nécessaire, on ne peut pas les imaginer en dehors du contrôle du juge ou dans des conditions qui pourraient concerner éventuellement la gestion même de ces réseaux mais là-aussi il importe que les opérateurs et les fabricants de ces technologies le disent.

C'est d'ailleurs l'occasion pour moi de dire que je crois tout à fait essentiel que les pouvoirs de la CNIL dans ce domaine soient étendus, la CNIL qui a été fondée il y a plus de 30 ans maintenant et qui est sensée jouer un rôle notamment sur la protection de la vie privée la protection des données personnelles en particulier quand

---

4 Rapport au parlement sur les exportations d'armement de la France en 2010 : http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics//114000643/0000.pdf
5 Al Jazeera espionné par Amesys : http://owni.fr/2011/12/14/al-jazeera-amesys-espionnage-spyfiles-libye/

on constitue des bases de données gagnerait énormément à voir étendre ses compétences dans le domaine de l'ensemble des libertés numériques, justement pour prévenir des atteintes comme celles qu'on voit poindre aujourd'hui en France, et c'est vrai qu'aujourd'hui nous avons beaucoup de difficultés, en dehors du travail que chacun peut faire là où il est, à prévenir et encadrer ces menaces. Voilà quelques mots que je voulais dire pour planter le décor de la table ronde d'aujourd'hui, pour introduire cette discussion à laquelle vous êtes tous invités à participer dans quelques instants. Donc trois intervenants qui vont lancer le débat, Jean-Marc Manach qui est journaliste notamment pour le site OWNI, qui a été avec Olivier Tesquet et d'autres, un de ceux qui ont mené ce travail d'investigation qu'OWNI a mené, en même temps que Mediapart le prenait aussi avec Fabrice Arfi par d'autres bouts ; Olivier Lorelli qui participe lui aussi à un site dédié au numérique qui s'appelle Reflets, et qui a beaucoup travaillé ces derniers mois sur cette question et notamment sur la Libye ; Jean-Marc Salmon qui est journaliste également, qui lui a regardé ce qui se passait en Tunisie et en Syrie notamment. Interviendrons donc ceux qui sont là si vous le souhaitez, d'autres qui doivent nous rejoindre dans la soirée, je pense que Fabrice Epelboin doit nous rejoindre également, Frédéric Martel, mon collègue Patrick Bloch qui est député de Paris avec qui on a beaucoup travaillé sur les questions du numérique et notamment dans la bataille d'Hadopi.

J'ai deux excuses à vous transmettre, j'avais invité les présidents des deux entreprises directement concernées, Bull et Qosmos. De la part de Bull j'ai obtenu de la part de son président, des excuses courtoises et une invitation à déjeuner. Donc j'accepte les excuses, mais je préfèrerai plutôt transformer l'invitation à déjeuner en une rencontre dans mon bureau au troisième étage, avec quelques autres parlementaires en guise de témoins. De la part de Qosmos mon invitation a été un peu tardive semble-t-il, donc là aussi j'ai les excuses de Qosmos à vous transmettre. Voilà, ça c'était pour détendre un peu l'atmosphère, je propose que Jean-Marc Manach commence, et puis ensuite Olivier.

M. Jean-Marc Manach, journaliste. (12 min 16 s). Bonsoir, pour essayer de résumer un petit peu ce qu'on a découvert, là je ne vais pas parler tout de suite d'Amesys ou de Qosmos mais de ces marchands d'armes de surveillance. Pendant trois mois on a travaillé avec Wikileaks sur des documents[6] et des plaquettes commerciales, du mode d'emploi, qui sont donnés par ces marchands d'armes à leurs clients potentiels. Un certain nombre de ces documents émanait d'un salon qui s'appelle ISS, qui a lieu tous les trois-quatre mois un peu partout dans le monde, à Kuala Lumpur, Washington, Prague etc., où les journalistes n'ont pas le droit de rentrer, et c'est un salon exclusivement dédié aux clients et aux fournisseurs de systèmes d'interception des télécommunications et de surveillance, c'est l'acronyme ISS. On s'est aperçu à cette occasion, que des systèmes, ce genre de systèmes qui jusqu'à la fin des années 1990 étaient a priori réservés à la NSA, à la DGSE, à la DRM, des services de renseignements militaires chargés de l'espionnage des télécommunications, depuis 2001 et l'explosion des systèmes de surveillance des télécommunications commencent à être de plus en plus vendus par des beaucoup plus petites sociétés[7] qui n'ont pas les mêmes rapports contractuels que les gros marchands d'armes -qui auparavant travaillaient avec les services de renseignements- et qui commencent à avoir comme client dans les salons ISS, on trouve aussi bien des représentants des polices municipales, donc la police municipale vient acheter des systèmes d'interception des télécommunications, ou de surveillance de l'Internet, on se demande pourquoi[8], à quel niveau la police municipale doit faire ça, que des gens qui effectivement viennent de pays pas démocratiques, peu démocratiques, voire de dictatures.

Donc c'est là où on a l'exemple typique depuis le printemps arabe et merci au printemps de nous avons ouvert les yeux en montrant à quel point les technologies occidentales pouvaient être vendues dans des pays dictatoriaux, ou peu démocratiques, et donc on a eu un changement d'échelle. C'est-à-dire que on savait depuis quelques années que la Chine et l'Iran notamment avaient utilisé, avaient acheté du matériel américain, du matériel allemand pour surveiller l'Internet dans leur pays, on ne savait pas du tout jusqu'à il y a quelques

6 Internet massivement surveillé : http://owni.fr/2011/12/01/spy-files-interceptions-ecoutes-wikilleaks-qosmos-amesys-libye-syrie/
7 La carte d'un monde d'espions : http://owni.fr/2011/12/01/spy-files-wikileaks/
8 Amesys, une entreprise innovante qui analyse (aussi) votre comportement : http://reflets.info/leweb-amesys-une-entreprise-innovante-qui-analyse-aussi-votre-comportement/

mois, que la Syrie la Libye, la Tunisie, avaient à ce point-là, un nombre de contrats importants avec des entreprises occidentales. Et ce qui est fou, c'est que quand le directeur de l'ISS, interviewé il y a quelque temps par le Wall Street Journal[9] qui lui demande : « *mais vous avez conscience que les systèmes que vous vendez peuvent éventuellement porter atteinte à l'intégrité physique voire à la vie de certains opposants politiques ?* » Et sa réponse c'est de dire : « *oui mais attendez, on est dans un libre marché, c'est légal, donc à partir du moment où c'est légal, nous on vend, il n'y a rien qui nous interdit de le faire* ». Et c'est exactement la réaction qu'a eu monsieur Samtmann qui est le responsable défense Amesys, quand il a accepté de répondre à une interview de France 2[10], parce que pendant très longtemps Amesys a refusé de répondre aux questions des journalistes, la réponse qu'il a donnée à la journaliste de France 2 qui lui a demandé : « *mais vous avez conscience que votre système pouvait, a pu servir à réprimer des défenseurs des droits de l'homme ?* » La réponse qu'il a donnée c'était de dire: « *oui mais c'est légal* », voilà.

Et donc j'en reviens là au communiqué de presse d'Amesys du 1er septembre dernier[11], qui est la seule chose qu'Amesys a produit, suite à la confirmation par le Wall Street Journal que Amesys était bien utilisé en Libye, il y a un passage qui est très intéressant dans le communiqué de presse qui dit : « *Amesys respecte toutes les lois nationales européennes et internationales* ». Et c'est vrai, il y en a pas, il n'y a pas de loi. C'est facile de respecter un cadre légal quand il n'y a pas de cadre légal. Et je pense que tout le problème aujourd'hui, c'est ça. C'est que Amesys une boîte française, Qosmos une autre boîte française, et c'est pareil pour des entreprises en Allemagne en Grande-Bretagne et aux Etats-Unis, ont le droit de vendre des systèmes de surveillance massifs d'espionnage, des outils de lutte informatique offensive, des chevaux de Troie (j'ai fait un autre article sur FinFisher notamment[12]), il y a cinq ou six entreprises au monde, dont une française, et FinFisher qui est une entreprise allemande ou anglaise je crois, qui vendent des chevaux de Troie, des outils de lutte informatique offensive pour espionner tel ou tel ordinateur, à partir du moment où l'ordinateur a été protégé par un certain nombre de mesures de sécurité. Donc quand ils ne peuvent pas espionner en clair ils ont aussi les moyens d'espionner ce qui est protégé. Le problème c'est que c'est légal, alors qu'est-ce qu'on peut faire avec ça ?

La réponse sera politique, la réponse commence à être politique au sens où Hillary Clinton a dit[13] que ce n'était pas normal que des démocraties aient vendu de tels systèmes à la Libye et à la Syrie, on a Neelie Kroes qui a fait une communication il y a deux jours[14], qui a lancé un projet qui vise à aider les cyber dissidents. Il y a quatre mesures pour aider les cyber dissidents, il y en a une, c'est de leur fournir des outils pour protéger les communications, mettre en place une sorte de système de communication distribuée qui serait à mi-chemin entre un Facebook et un Wikileaks si je résume un petit peu ce qu'elle veut mettre en place, pour surveiller l'utilisation de matériel d'interception des télécommunications et de surveillance de l'Internet dans les pays pas ou peu démocratiques, une sorte d'observatoire pour aider les démocraties à aider les démocrates.

Mais par contre à ce jour on n'a eu aucune mesure politique au niveau national ou international, pour arriver à rajouter ces outils de surveillance des télécommunications dans la liste du matériel de guerre, au sens où il y a l'accord de Wassenaar[15] au niveau international, il y a la CIEEMG[16] au niveau français, qui définissent qu'est-ce qu'une arme dont l'export doit être validé par des commissions adéquates[17]. Alors quand on a interrogé la CIEEMG, donc la commission interministérielle qui est placée sous l'auspice de Matignon, *est-ce que vous avez autorisé Amesys à vendre son système Eagle[18] d'interception des télécommunications à la Libye ?*[19] La CIEEMG

9 Document Trove Exposes Surveillance Methods : http://online.wsj.com/article/SB10001424052970203611404577044192607407780.html
10 Le logiciel espion vendu à Kadhafi devait "chasser le pédophile", pas l'opposant : http://www.francetv.fr/info/la-societe-francaise-qui-a-aide-kadhafi-a-traquer-ses-opposants-se-defend_35639.html
11 Communiqué Amesys : http://www.wcm.bull.com/internet/pr/new_rend.jsp?DocId=673283&lang=fr http://www.scribd.com/doc/63801804/AmesysCP
12 Un gros requin de l'intrusion : http://owni.fr/2011/12/12/finfisher-cheval-de-troie-gros-requin-intrusion-surveillance/
13 Conference on Internet Freedom : http://www.state.gov/secretary/rm/2011/12/178511.htm
14 Stratégie numérique: Mme Kroes invite M. Karl-Theodor zu Guttenberg à promouvoir la liberté d'expression sur l'internet au niveau mondial : http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/1525&format=HTML&aged=0&language=FR&guiLanguage=en
15 The Wassenaar Arrangement : http://www.wassenaar.org
16 Commission Interministérielle d'Étude des Exportations de Matériels de Guerre : http://www.defense.gouv.fr/das/maitrise-des-armements/node_73891/le-controle-des-exportations
17 Rapport d'information n° 2 (2007-2008) de MM. François MARC et Michel MOREIGNE, fait au nom de la commission des finances, déposé le 2 octobre 2007 : http://www.senat.fr/rap/r07-002/r07-002.html
18 Eagle Operator Manual : http://www.scribd.com/doc/74391831/Eagle-Operator-Manual

nous a dit: *ben non, parce que ce n'est pas dans le décret*. De fait, Amesys, anciennement I2E, a été créée comme entreprise de guerre électronique, et la guerre électronique ce sont des militaires qui espionnent les communications d'autres militaires. Mais les militaires n'utilisent pas Internet, ils utilisent d'autres systèmes de télécommunication. Donc la guerre électronique, essentiellement, ça va être la surveillance du spectre électromagnétique, pas la surveillance de l'Internet en tant que tel. Et donc ils ont joué sur les mots pour dire que des outils d'interceptions des télécommunications et de surveillance de l'Internet ce ne sont pas des outils de guerre électroniques, donc ce ne sont pas des armes, donc on a le droit de le vendre. D'ailleurs c'est ce qu'a répondu le ministre des affaires étrangères interrogé par un journaliste du Monde[20], il répond : *la CIEEMG n'a pas à délivrer d'autorisation, car cela ne fait pas partie des produits concernés par le décret*.

Au niveau européen, on a eu fin septembre un projet de directive qui a été adopté par les eurodéputés[21] et qui a fait l'objet d'âpres négociations et où visiblement d'après les informations à ma disposition, c'était un projet qui date d'il y a environ deux ans, qui visait à rajouter à la liste des armes dont l'export doit être sévèrement contrôlé, les outils d'attaque informatique qui permettent d'attaquer quelqu'un, un pays, attaquer une entreprise, et les outils de surveillance de l'Internet et d'interception des télécommunications. Visiblement suite à la pression d'un certain nombre de pays qui vendent ce genre d'outils, les outils d'attaque ont été retirés de la liste, et quant aux outils qui visent à intercepter les télécommunications, le lobbying a été tel que, il sera, si la directive est réellement adoptée, il sera légal de vendre du matériel, il faudra demander l'autorisation après, une fois que le matériel a été vendu. Ce qui est une conception de la régulation que je trouve assez particulière.

Donc pourquoi on est dans cette situation ? Si on regarde la carte des entreprises[22] qui commercialisent ce genre d'outils d'interception des télécommunications, enfin ceux que j'appelle les marchands d'armes de surveillance, il y en a 32 aux États-Unis, 18 ou 17 en Grande-Bretagne, 15 en Allemagne, 8 en France, 10 en Israël et 7 en Italie, et après ça tombe à trois. L'essentiel de ces marchands d'armes de surveillance sont dans des pays européens ou sont aux États-Unis, c'est un marché énorme. Le PDG d'ISS expliquait que c'est un marché qui est parti de grosso modo de zéro en 2001 et c'est lui qui le dit[23], qui est estimé aujourd'hui à 5 milliards de dollars par an. La France pour ne parler que d'elle, via le fonds stratégique d'investissements, a investi dans Bull en août dernier[24] et dans Qosmos en septembre[25]. Le PDG de Bull a reçu la Légion d'honneur de la part du ministre de la défense[26] en juillet dernier. Ce sont des technologies stratégiques considérées comme stratégiques par la France, par le gouvernement français, au point que le gouvernement français a investi dans ces technologies. Le moins que l'on puisse attendre d'un gouvernement, d'une démocratie comme la France, est que s'il investit et s'il est au conseil d'administration de ces technologies, non seulement il fasse usage de son droit de regard au conseil d'administration, mais qu'il change la loi pour éviter des scandales comme celui dont la France est entachée aujourd'hui, car au lieu d'être considéré uniquement comme le pays qui a contribué à aider la Libye, on est aussi considéré aujourd'hui comme le pays qui a contribué à espionner les dissidents libyens.

Et pour ceux qui n'ont pas suivi, dans la liste des dissidents libyens que j'ai sortis, donc qui ont été espionnés[27], il y en a un qui est aujourd'hui ambassadeur de Libye à Londres, et un autre ministre de la culture en Libye. Donc ce n'était pas des petits. Et aujourd'hui le Wall Street Journal a sorti un article[28] où on voit qu'ils ont aussi

---

19 Ecoutes en Libye : un officier formateur français témoigne sur le site du Figaro : http://www.arretsurimages.net/contenu.php?id=4272
20 La France a aidé Kadhafi à espionner son pays (Canard/Monde) : http://www.arretsurimages.net/vite.php?id=11974
21 Résolution législative du Parlement européen du 27 septembre 2011 sur la proposition de règlement du Parlement européen et du Conseil portant modification du règlement (CE) n° 1334/2000 instituant un régime communautaire de contrôles des exportations de biens et technologies à double usage (COM(2008)0854 – C7-0062/2010 – 2008/0249(COD)) : http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2011-0406+0+DOC+XML+V0//FR
22 La carte d'un monde d'espions : http://owni.fr/2011/12/01/spy-files-wikileaks/
23 Document Trove Exposes Surveillance Methods : http://online.wsj.com/article/SB10001424052970203611404577044192607407780.html
24 BULL : le FSI prend plus de 5% du capital : http://fr.finance.yahoo.com/actualites/BULL-FSI-prend-5-capital-aof-3715559081.html
25 Le FSI investit dans Qosmos : http://www.artesi.artesi-idf.com/public/article.tpl?id=24211
26 Décret du 13 juillet 2011 portant promotion et nomination au grade de chevalier : http://www.legiondhonneur.fr/shared/fr/promo/lh/jo110713llhdecret14juillet.html#3
27 Réfugiés sur écoute : http://owni.fr/2011/12/01/amesys-bull-eagle-surveillance-dpi-libye-wikileaks-spyfiles-kadhafi/
28 Life Under the Gaze of Gadhafi's Spies : http://online.wsj.com/article/SB10001424052970203764804577056230832805896.html

espionné un journaliste d'Al Jazeera[29], qui est un des rares journalistes libyens qui prenait le risque de rester en Libye pour pouvoir de l'intérieur, couvrir les affaires libyennes, et qui a failli en mourir. Donc voilà, il y a ça. Et la question qui va se poser après, c'est que, quand bien même on rajoute ces outils à la liste des armes qui devraient être contrôlées par le CIEEMG, vu les rapports qu'entretenait à l'époque la France avec la Libye, en 2007, je pense que la vente aurait été autorisée. Vu qu'on sait très bien, ça c'est Mediapart qui l'a montré[30], que le contrat passé par Ziad Takieddine était négocié parce que Sarkozy, Brice Hortefeux et Claude Guéant voulaient rapprocher la France et la Libye. Donc est-ce que c'est normal ou moral, de donner une autorisation gouvernementale pour la vente d'un tel outil à une dictature ? Je sais que j'ai posé la question également à Matignon, est-ce que vous avez autorisé la vente du 4X4 sécurisé et du logiciel de chiffrement CryptoWall[31] qui ont aussi été vendus à la Libye ?[32] Parce que tous les deux figurent dans la liste CIEEMG des produits interdits à l'export. J'ai eu zéro réponse de Matignon, zéro réponse de la CIEEMG.

Autre question, on sait que Amesys a vendu ces technologies notamment au Maroc[33] au Qatar[34], et à un certain nombre d'autres pays qui sont pas à proprement parler des dictatures, sauf que on sait que là-bas la liberté de la presse elle n'existe pas vraiment. Donc la question c'est, est-ce que c'est uniquement de considérer ça comme des armes, sauf que si on vend un char d'assaut à Kadhafi il y a peu de chance qu'il s'en serve pour tuer des populations civiles, alors que si on vend des armes de surveillance, des technologies de surveillance on sait que les premières cibles ça va être les civils. Ce sont des technologies duales, et M. Vannier le PDG de Amesys devenu PDG de Bull expliquait que quand il a créé Amesys qui était spécialisé à l'époque dans le marché de la défense, il s'est dit il y a un boulevard en matière de sécurité. Et là ce qu'on voit c'est que ce sont des technologies qui étaient initialement réservées aux professionnels de l'armement de la défense, qui aujourd'hui sont utilisées en termes de sécurité et donc visent des civils. Je ne sais pas s'il est suffisant de rajouter ces technologies-là à la liste de la CIEEMG.

Deuxième chose, en France on a une commission qui est la commission R226[35] qui régit tout achat ou toute utilisation de matériel d'atteinte à la vie privée, d'interception des télécommunications. Je viens de vérifier c'est une commission qui dépend de l'ANSSI, qui est présidée par l'ANSSI qui dépend de Matignon, il n'y a pas la CNIL. Il n'y a pas de représentant de la CNIL dans cette commission qui vise pourtant explicitement à protéger la vie privée et à délivrer ou pas des autorisations. Dans le cadre de mon enquête je me suis aperçu, j'ai découvert qu'il y avait sept systèmes[36] qui ont été vendus par Amesys ces dernières années au ministère de l'intérieur et de la défense. Ni le ministère de l'intérieur, ni celui de la défense ni Matignon ni l'ANSSI n'ont répondu à ma question, moi je voulais juste savoir à quoi ça sert. Et qu'est-ce qui me garantit qu'effectivement ce n'est pas utilisé pour espionner des civils, comment vous pouvez rassurer l'opinion publique sur le fait que vous avez acheté pour plusieurs millions d'euros de systèmes d'interception massive des télécommunications.

Donc on touche là je pense quelque-chose qui est éminemment politique, qui est un petit peu « *touchy*[37] » parce que effectivement ça ne fait pas une très bonne image de certaines entreprises françaises, voire du gouvernement vu qu'on sait qu'il est impliqué. Je pense qu'il y a un vrai débat, il faut qu'il y ait un débat public, est-ce qu'il est normal en démocratie qu'on puisse autoriser ça, et si ce n'est pas normal, jusqu'où il faut aller. Et je pense que ça ne suffit pas de dire que ce sont des armes de guerre. Ça ne suffit pas de les rajouter dans la liste du matériel interdit à l'export. Parce que ça permettra de toute façon l'espionnage de civils, et moi ce que j'ai vu, pour l'instant les seules personnes dont on ait la preuve qu'elles ont été espionnées grâce aux logiciels

29 Al Jazeera espionné par Amesys : http://owni.fr/2011/12/14/al-jazeera-amesys-espionnage-spyfiles-libye/
30 Sarkozy-Guéant: le grand soupçon libyen : http://www.mediapart.fr/journal/international/280711/les-documents-takieddine-sarkozygueant-le-grand-soupcon-libyen
31 IE2 CRYPTOWALL le meilleur moyen de sécuriser vis échanges : http://www.scribd.com/doc/61134860/IE2
32 Le droit français tordu pour Kadhafi : http://owni.fr/2011/09/28/amesys-libye-kadhafi-droit/
33 Maroc : Le meilleur ami de la France se met au DPI grâce à Amesys, la filiale de Bull : http://reflets.info/maroc-le-meilleur-ami-de-la-france-se-met-au-dpi-grace-a-amesys-la-filiale-de-bull/
34 Qatar : Le Finger tendu bien haut d'Amesys : http://reflets.info/qatar-le-finger-tendu-bien-haut-damesys/
35 Commission nationale de contrôle des interceptions de sécurité : http://www.legifrance.gouv.fr/affichTexteArticle.do?idArticle=LEGIARTI000006421121&cidTexte=LEGITEXT00000607778
36 Amesys surveille aussi la France : http://owni.fr/2011/10/18/amesys-surveille-france-takieddine-libye-eagle-dga-dgse-bull/
37 « Touchy », Délicat, sensible (en parlant d'un sujet) : http://fr.wiktionary.org/wiki/touchy

d'Amesys, c'est pas des terroristes, c'est des figures historiques de l'opposition, donc des gens qui ont maintenant des responsabilités dans l'appareil politique libyen, et ce sont les journalistes, et des avocats, et des défenseurs des droits de l'homme et des fonctionnaires américains. Il y avait des gens qui étaient payés par le congrès pour donner de l'argent du congrès américain à des dissidents libyens, ils ont été espionnés, parce qu'on a découvert également, c'est que, ces systèmes-là permettent non pas d'espionner seulement une personne, mais les contacts des contacts de cette personne. Donc là réellement ça va bien plus loin que de prendre une arme et de tirer sur quelqu'un qui en face a une arme, c'est vraiment l'espionnage de la population civile.

M. Olivier Laurelli, cofondateur Reflets.info. (26 min 09 s). J'ai travaillé un petit peu sur ces dossiers, je travaille à ça depuis 2008-2009. On a mis un petit peu les bouchées doubles l'été dernier avec les collègues de *Reflets.info*, suite à des informations qu'on a obtenues concernant justement les ventes de systèmes d'écoutes globales, donc là je parle du système qui a été vendu notamment à la Libye. Un système d'écoute globale, c'est-à-dire un système qui est conçu pour écouter l'ensemble des communications d'un pays et non pas, comme on l'avait lu dans le communiqué d'Amesys, une fraction des communications de la population. On était bien dans un système d'écoute généralisée de tout le pays, donc la journaliste du Wall Street Journal qui s'est rendue sur place et qui a découvert à la fois le matériel, à la fois les dossiers d'interceptions avec les transcriptions, donc si vous voulez très vite tous nos soupçons ont été confirmés. Je retrace un petit peu l'historique de comment on en est arrivé à plancher sur ces dossiers.

Un petit peu plus récemment on a travaillé[38] avec groupement d'activistes qui s'appelle Telecomix[39] qui est un groupement d'origine suédoise mais qui regroupe des gens du monde entier, sur un autre cas qui était le cas de la Syrie et d'une entreprise américaine qui s'appelle Blue Coat. Blue Coat qui avait livré ce qu'on appelle des « *appliances*[40] », c'est-à-dire des espèces de gros boitiers dans lesquels on s'amusait à router le trafic, à interdire l'accès à certains sites, et éventuellement dans certains cas, sur des sites de type Facebook, Gmail, tous les sites dans lesquels on met nos mots de passe et dans lesquels on fait transiter toutes nos données personnelles, redirigeaient le trafic sécurisé, c'est-à-dire les sessions *https* quand vous avez le petit cadenas dans votre navigateur, sur la même page, mais qui était non chiffrée[41]. La finalité de cette petite redirection qui ne devait pas interpeler beaucoup de monde, sauf les gens qui sont un petit peu aguerris à ce genre de chose, était de récupérer simplement les informations personnelles, donc les mots de passe et d'avoir accès à des comptes.

On a suite à ça, mis la main sur des journaux de connexion qui émanaient de ces matériels, on a publié[42] sur *Reflets.info* l'intégralité de ce qu'on a récupéré, c'était sur une période de deux-trois mois je crois, c'était pas énorme, ça représentait quand-même 54 Go de fichier texte, on parle de fichier texte, donc c'était 54 Go de traces de connexion de l'ensemble de la population syrienne, où on voyait des mesures de blocage sur certains sites et donc cette petite redirection qui nous ont pas mal interpelés. Suite à cette publication, il devenait difficile pour l'entreprise incriminée donc l'entreprise américaine qui s'appelle Blue Coat de nier cet état de fait, ce qu'elle a pourtant fait au début en disant non, non, on a pas contourné l'embargo, parce qu'il y a un embargo américain sur les ventes à la Syrie, donc ils ont commencé par nier[43] puis on a quand-même appris un petit peu après, qu'il y a eu 22 « *appliances* » qui ont quand-même été livrées à la Syrie[44]. Donc ils étaient tout-à-fait au courant.

---

38 Quand internet ne laisse pas tomber les citoyens Syriens : http://reflets.info/opsyria-quand-internet-ne-laisse-pas-tomber-les-citoyens-syriens/
39 Geek Politics Interview, by Dancing Dog Productions - Telecomix : http://vimeo.com/34021791
40 Appliance (Boîtier), appareil dédié à une fonction bien précise, par opposition à un micro-ordinateur généraliste : http://www.journaldunet.com/solutions/systemes-reseaux/appliance/
41 BlueCoat maître artisan de la censure syrienne : http://reflets.info/opsyria-bluecoat-maitre-artisan-de-la-censure-syrienne/
42 Syrian Censorship Logs (Season 3) : http://reflets.info/opsyria-syrian-censoship-log/
43 Pourquoi #BlueCoat a menti ? : http://reflets.info/opsyria-pourquoi-bluecoat-a-menti/
44 BlueCoat admet maintenant la présence de ses produits sur le sol syrien : http://reflets.info/opsyria-bluecoat-admet-maintenant-la-presence-de-ses-produits-sur-le-sol-syrien/

Il faut savoir qu'ils ont menti en plus de manière assez éhontée, parce que ce genre de boitiers non seulement ils sont tracés, mais en plus de ça, quand vous les connectez la première chose qu'ils font c'est de se connecter chez papa pour aller faire leur mise à jour. Donc ils ne pouvaient pas si vous voulez, en tant que fabricant et, on va dire, tenancier un petit peu du site web qui distribue les micro-logiciels qui sont intégrés dans ces boitiers, ne pas savoir qu'il y avait sur le territoire syrien leurs « *appliances* » qui servaient massivement à censurer les sites web. Donc le cas de Blue Coat[45] est pour nous assez emblématique parce qu'on s'est retrouvé avec une masse d'informations assez colossale qui était vraiment un instantané de la censure de l'ensemble d'un pays. Donc si vous voyez que ceci existe sur un pays comme la Syrie qui est effectivement un petit peu agité comme en ce moment, rien ne vous interdit de penser qu'on va retrouver ça dans d'autres pays. Comme le disait Jean-Marc ça peut être des dictatures, ça peut être des pays un petit peu moins démocratiques que l'image qu'on s'en fait.

Le cas de la Libye lui est encore plus rigolo, Jean-Marc faisait référence à la date de 2007, année à laquelle Kadhafi a été reçu avec les honneurs de la République, il faut savoir que la vente du système Eagle à la Libye date pas de 2007, elle date de 2006, donc un an avant déjà[46]. On a publié à l'instant un article sur *Reflets.info* qui va vous faire état de faits qui sont que quelques jours avant que ça pète un petit peu en Libye, c'est -à-dire le 17 février dernier, le directeur d'Amesys Monsieur Vannier était présent sur le territoire Libyen pour vendre le même système qu'il a vendu au Qatar très très récemment et qui fait scandale en ce moment. Donc vous aller les trouver assez facilement enfin vous allez voir il y a des prélèvements de retraits de faux-frais de 3000 Euros, qui tombent pas en 2006 qui tombent là du début de l'année[47]. Donc quand Amesys va déclarer que non, on a vendu ça en 2006 et on n'a pas assuré de support ni rien, bon ça c'est faux, on sait qu'il y a un support qui a été assuré, et on sait que les relations commerciales ont perduré si vous voulez, dans le temps. Elles ont perduré à un point tel que ben, juste quelques jours avant la révolution les gens d'Amesys étaient sur place encore pour essayer de vendre un système on va dire, « *upgradé* », une solution un petit mieux dimensionnée aux usages. On a parlé des écoutes Internet, il faut savoir que le système d'Amesys n'écoutait pas qu'Internet, il écoutait également les communications satellitaires[48], notamment d'un satellite qui s'appelle Thuraya qui est un peu le mode de communication des rebelles, par les dissidents, ces communications étaient écoutées, « *monitorées* », et évidemment tout ça était archivé[49].

Pour revenir un petit peu plus techniquement sur ce type de solution, je vais repartir un petit peu sur la technologie elle-même, parce que la défense d'Amesys ça va être de vous dire, écoutez, nous on vend des balles on n'appuie pas sur la gâchette. C'est un argument que vous allez retrouver chez tous les revendeurs d'armes en général[50]. Cet argument sur du DPI c'est un petit peu culotté parce que le DPI si vous voulez est très comparable à l'énergie nucléaire, au nucléaire. C'est un petit peu ce qu'on appelle le nucléaire d'Internet dans notre petit jargon. Pourquoi le nucléaire de l'Internet? parce que vous allez pouvoir en faire des choses très très bien, comme du « *monitoring* », de la sécurité, c'est-à-dire essayer d'éviter des vagues virales, des propagations virales sur un réseau d'opérateur, vous allez pouvoir faire des choses magnifiques avec ce genre de technologie, mais dans « *Deep Packet Inspection* » il y a la définition même du mot qui dit que ça inspecte en profondeur vos communications, inspecter en profondeur ça veut dire que ça lit ce qu'on appelle la charge utile d'un paquet sur Internet ce qu'on appelle le « *payload* », cette définition même au sens de l'article 226.15[51] du code pénal, c'est une atteinte au secret de vos communications.

C'est-à-dire que déployer cette technologie pour un autre usage, un autre sens, après avoir pas mal bossé sur le sujet, pour une autre utilisation que les interceptions légales, c'est-à-dire opérées sur la demande d'un juge,

---

45 U.S. Firm Acknowledges Syria Uses Its Gear to Block Web : http://online.wsj.com/article/SB10001424052970203687504577001911398596328.html
46 Amesys : Kadhafi augmented : http://reflets.info/amesys-kadhafi-augmented/
47 Amesys : un peu de fraîche pour la Libye : http://reflets.info/amesys-de-la-fraiche-pour-la-libye/
48 Glint_EN : http://www.scribd.com/doc/63653409/Glint-EN
49 Les grandes oreilles libyennes d'Amesys écoutaient aussi les satellites : http://reflets.info/les-grandes-oreilles-libyennes-damesys-ecoutaient-aussi-les-satellites/
50 Le Deep Packet Inspection est-il une arme ? Rencontre avec Qosmos : http://techtoc.tv/event/1079/libertes-et-devoirs-numeriques/nos-droits-numeriques/le-deep-packet-inspection-est-il-une-arme
51 Article 226-15 : http://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006070719&idArticle=LEGIARTI000006417954&dateTexte=20090620

peut être considéré comme abusif[52]. Il faut savoir aujourd'hui que cette technologie est utilisée par exemple par les réseaux d'opérateurs 3G pour de la facturation[53]. C'est employé également au cœur de réseaux par certains opérateurs pour pouvoir différencier le trafic professionnel du trafic grand public[54]. Donc il y a tout un tas d'utilisations, dont certaines qu'on voit arriver, qui commencent à être un petit peu inquiétantes.

Monsieur le Député a beaucoup travaillé sur les questions d'Hadopi, je vous avouerai que nous, notre grosse frayeur aujourd'hui, c'est de voir cette technologie utilisée pour faire de la reconnaissance de contenus, et épurer tout ce qui n'est pas contenus on va dire « légaux », ça reviendrait à mettre des pseudo-douaniers virtuels dans les routeurs des opérateurs. C'est-à-dire qu'une intelligence artificielle pourrait décréter que tel fichier qui possède une extension *.AVI* et qui pèse 700 Mo est forcément un fichier piraté. Non, ça va très très loin si vous voulez, à partir de ce moment-là, qu'est-ce qui va se passer? C'est que, voyant transiter ce fichier sur le réseau, le routeur va dire, je ne le laisse pas passer parce qu'il pèse 700 Mo et que c'est un *.AVI* donc c'est un forcément un fichier pirate. Donc là on parle vraiment de censure appliquée à l'ensemble des communications du réseau, ce qui est quelque-chose qui est tout-à-fait faisable techniquement malheureusement, il faut savoir qu'Internet n'est pas si décentralisé qu'on le dit. Il y a très peu d'opérateurs en France qui ont un réseau complètement *acentré* [décentralisé]. Il y a toujours des terminaisons dans lesquelles on est capable d'écouter en fait des Térabits de bande passante. Le DPI est efficace jusqu'à 40 Gigabits mais en répartissant bien tous ces matériels on arrive vraiment à intercepter beaucoup de communications.

Il y a un autre usage qui est fait de cette technologie qui est la publicité. Très récemment, Orange annonçait une offre, qui nous a inquiété, mais vraiment inquiété[55], qui s'appelle Orange préférence[56]. C'est une expérimentation qui a été lancée aux abonnés, sur « *Opt-In*[57]», c'est-à-dire que l'abonné va s'inscrire, va souscrire à cette offre, et alors c'est assez rigolo parce que c'est l'abonné qui va demander à ce qu'on lui administre de la publicité. Donc déjà pourquoi pas, je serais curieux de connaître les chiffres d'Orange, d'abonnés qui ont souscrit à cette offre, dont le concept est de surveiller les surfs de l'abonné, il y a pas d'informations apparemment qui sont stockées parce que ça a été sous l'égide bienveillante de la CNIL qui a cautionné cet usage[58] qui à moi me paraît complètement hallucinant. Donc on étudie les sites que vont visiter les internautes, et une fois qu'on a bien étudié tout ce qu'ils visitent et bien on leur administre de la pub un tout petit peu plus ciblée. A partir de ce moment-là, quand vous voyez ce genre de technologie arriver pour des usages publicitaires, vous pouvez déjà commencer à vous demander s'il n'y a pas une dérive qui est opérée.

Ensuite, je parlais d'interceptions légales, on peut très bien opérer également des interceptions illégales. Une fois qu'on a ce type de sondes, ce type de matériel, il suffit d'une petite mise-à-jour logicielle pour opérer des écoutes sur des milliers de communications, des milliers de connexions. En regardant un petit peu les pays dans lesquels Amesys avait déployé ses solutions on a repéré un câble sous-marin, et puis on s'est posé des questions et on s'est fait un petit scénario de fiction[59] et on a commencé à se demander s'il était possible pour Amesys, ou pour des services, d'écouter des communications de ressortissants français, les communications françaises des français, depuis les pays où ces solutions ont été déployées. Et bien figurez-vous que techniquement, rien n'empêche de faire ça. On a un exemple parfait, qui a été évoqué par Jean-Marc, qui est à l'écoute justement de ressortissants Libyens qui n'étaient pas sur le territoire Libyen. Il faut savoir que les communications forcément ça marche dans deux sens, il y a deux interlocuteurs au minimum, donc il peut y avoir des gens qui ne sont pas dans le pays. Mais il y a plus vicieux que ça. C'est-à-dire que deux français qui vont pouvoir communiquer entre eux, qu'est-ce qui va empêcher un opérateur de lancer une règle de routage sur un point donné du réseau, pour que l'écoute s'effectue en dehors du territoire ? Là encore, la magie du

52 Les mystérieux screenshots d'Amesys : des écoutes sauvages en plein Paris ? : http://reflets.info/amesys-ecoutes-sauvages-paris-champs-elysees/
53 Orange et le Deep Packet Inspection sur les réseaux mobiles : http://reflets.info/orange-nokia-siemens-deep-packet-inspection/
54 Orange va expérimenter du QoS data différenciée pour les entreprises : http://reflets.info/orange-va-experimenter-du-qos-data-differenciee-pour-les-entreprises/
55 Deep Packet Inspection : Orange souhaite vous espionner avec votre consentement : http://reflets.info/deep-packet-inspection-orange/
56 Panel Orange Préférences : http://www.orange.fr/bin/frame.cgi?u=http%3A//privacy.orange.fr/presentation.do%253Ffamily%253Dconsent
57 Orange Préférences : le Deep Packet Inspection en Opt-In : http://reflets.info/orange-preferences-le-deep-packet-inspection-en-opt-in/
58 Quand la CNIL fait de la publicité pour le Deep Packet Inspection d'Orange : http://reflets.info/quand-la-cnil-fait-de-la-publicite-pour-le-deep-packet-inspection-dorange/
59 Et si… on était tous libyens ? : http://reflets.info/et-si-on-etait-tous-libyens/

protocole TCP/IP fait que c'est tout-à-fait faisable et que c'est tout-à-fait facile à faire. Et on peut le faire sur des milliers de connexions.

Donc aujourd'hui si vous voulez on se pose encore plus de questions que quand on a commencé à travailler sur le dossier Amesys, et on commence à appréhender un petit peu ce marché de la surveillance comme quelque chose d'assez malsain. Il y a quelque-chose qu'on ne s'explique pas encore sur le cas libyen, qui était la présence de la direction du renseignement militaire pour aider au déploiement de cette technologie sur le territoire. Là encore je pense qu'il y a eu des questions de parlementaires qui ont été posées dans ce sens, il y a toujours pas de réponse, donc c'est ce que vous disiez, il y a une dizaine de questions de parlementaires qui sont restées à ce jour sans réponse. Donc la présence de la DRM pour nous est un signe d'inquiétant. On sait que la direction des Services de Renseignent Militaire était sur place et a vraiment aidé au déploiement là-bas. Est-ce que c'était pour écouter uniquement des ressortissants libyens ou est-ce que c'était également pour mettre en place un système en « *Remote* » d'écoute de ressortissants français ? On peut se poser tout un tas de questions, techniquement il n'y a rien qui nous empêche de penser à tout ça.

M. Christian Paul, député. (39 min 08 s). Merci Olivier, Jean-Marc.

M. Jean-Marc Salmon, chercheur. (39 min 17 s). Oui bonjour, je suis chercheur, même s'il m'arrive à l'occasion de faire des commentaires dans la presse. Je suis affilié dans un groupe de recherche chez Tos qui appartient à l'institut Télécom, et d'ailleurs, c'est dans le cadre de ces activités de recherche qu'au moment de la révolution tunisienne, comme il y avait tout un tas de questions qui se posaient… On va dire, pour tracer assez rapidement le tableau intellectuel des débats que nous avons : il y a depuis longtemps un débat, une opposition, des polémiques entre disons des cyber-optimistes et des cyber-pessimistes ou entre des cyber-critiques et des cyber-béats, enfin bon peu importe. Grosso modo sur la politique internet il y a d'un côté des gens qui ont soutenu qu'au fond chaque innovation technologique était une source de libération et que donc on aurait une révolution Twitter, on aurait une révolution Facebook, on aurait une révolution Google, et cætera… et d'ailleurs très souvent dans les papiers de recherche il est au Moyen-Orient, voilà, il y a toute une littérature là-dessus qui est tout à fait traçable. Et puis on a inversement des gens qui insistaient sur le fait qu'au contraire les dispositifs internet étaient des dispositifs qui permettaient aux États beaucoup plus de contrôles qu'avant et que c'était donc qu'une illusion de penser qu'Internet pouvait aider la révolution. Donc c'était pour dire qu'intellectuellement le débat où on est là en ce moment c'est un débat qui nous intéresse, qui a lieu depuis longtemps, et le printemps arabe a modifié les termes dans lesquels on appréhende le débat à mon avis, ça l'amène à de nouveaux horizons.

Nous, je suis parti là-bas pour voir « *c'est Facebook, c'est pas Facebook* », tout ça ; j'avais déjà vu un papier d'Epelboin sur un peu les techniques de surveillance d'Internet[60] en Tunisie[61], voilà, c'était assez vague, hein, c'était assez vague, et je vois des gens, tout reste vague, et alors finalement je vois des gens à un niveau important dans le système transitoire, qui sont des gens de la… des hautes instances, vous savez on est en Tunisie pendant la transition, et il y a le gouvernement qui fait les affaires courantes et puis il y a tous les partis d'opposition et tous les opposants qui sont réunis dans les hautes instances de la révolution et en fait c'est eux qui vont décider de la date des élections, du mode de scrutin, qui sont des instances très politiques. Bon, on est en train de parler de la révolution, je leur dit « mais alors finalement cette surveillance d'internet ? » ; et alors il y a une femme, elle me dit « écoute, quant aux gens du gouvernement, tu leur dis *Bon mais alors la surveillance d'internet*, ils prennent un air offusqué en disant *mais comment? De quoi vous nous soupçonnez ?* » Etc. Autrement dit, même les gens, qui avaient été dans l'opposition influente qui est en droit de poser des questions, ils n'avaient pas de réponses. Je pense qu'on n'a d'ailleurs toujours pas de vraies réponses sur le système qui a été mis en place à l'époque de Ben Ali.

60 Zaba le Geek : Do be Evil : http://www.fhimt.com/2011/12/01/zaba-le-geek-do-be-evil/
61 Ammar 404 : les dessous de la société de la surveillance dans la Tunisie de Ben Ali : http://www.fhimt.com/2011/12/16/ammar-404-les-dessous-de-la-societe-de-la-surveillance-dans-la-tunisie-de-ben-ali/

Alors je leur dis : « Bon, enfin, tout ça, c'est préoccupant, je voudrais bien trouver quelqu'un qui connaisse ». Et donc le lendemain quelqu'un m'appelle et me dit « Bonjour, machin m'a dit de vous appeler, voilà. Si vous voulez cette après-midi on va voir un responsable de la sécurité informatique » Bon, j'annule mes rendez-vous, je dis « Bien sûr, allons-y ». Voilà. Alors, c'est intéressant, parce que d'abord on est dans le monde… ben voilà, il faut donner des garanties de secret, d'anonymat, que mes voisins doivent connaître, évidemment je lui ai dit *tout est en sécurité, votre nom ne sera jamais prononcé*, etc. mon interlocuteur est parti au café bien évidemment, il n'a pas assisté à l'entretien. Bon, et puis une fois que tout ceci est fait, qu'est-ce qu'il m'apprend, il m'apprend les dispositifs techniques. Il me dit *c'est simple, il y a une plate-forme, et cette plate-forme elle a été acquise en 87-88*, pardon, en 2007-2008 *pour monitorer toutes les communications qui passent par internet. Parce qu'il fallait voir avec la montée en puissance de Facebook tout ce qui pouvait passer par Facebook*. Alors en point d'histoire ici, c'est un point important quand on rentre dans les questions concrètes des pays arabes, les communications Facebook en 2008, Ben Ali veut les arrêter au mois d'août. Il les arrête, et les États-Unis interviennent, et finalement Ben Ali cède après trois semaines, et il rétablit les communications Facebook, et je pense que le timing doit donner à penser que au fond, il se disait que puisqu'il venait d'acquérir, ou qu'il était en train d'acquérir ou qu'il allait acquérir demain matin ce système-là, il serait tranquille.

Parce que Ben Ali, à la différence des autres dictateurs arabes est un fan d'informatique, donc il sait ce qu'il fait à la différence des autres. Ce n'est pas un sous-fifre qui prend les décisions importantes sur l'informatique en Tunisie, c'est Ben Ali. Voilà. Bon, à côté de ça, je comprends qu'il y a un montage, il y a deux sociétés… il y a une autre société qui fournit des logiciels, qui sont des logiciels complémentaires on va dire, il ne veut pas me donner les noms, donc je sais toujours pas les noms, donc les noms des sociétés qui ont travaillé en Tunisie ne sont toujours pas connus à ma connaissance. Voilà. Mais je pense qu'à la vitesse où ça va, on va bientôt finir par voir sortir des choses.

Intervenant non reconnu. (44 min 37 s). [Commentaire inaudible]

M. Jean-Marc Salmon, chercheur. (44 min 39 s). Ah ben voilà, ça m'avait échappé. C'est qui alors ?

Intervenant non reconnu. (44 min 42 s). [Commentaire inaudible]

M. Jean-Marc Salmon, chercheur. (44 min 43 s). Bon, on en parlera dans le débat tout à l'heure. Donc, donc voilà. Donc je me dis qu'il y a à faire, voilà, que le sujet est intéressant tout ça. Donc qu'est-ce que je voudrais dire ? D'abord, on voit bien, c'est un outil de police. Comme je suis chercheur, j'ai un peu tendance à faire attention aux mots. C'est d'abord un outil de police, ce n'est pas un outil de guerre. La police de Ben Ali, elle fiche les gens comme ça, elle les suit, elle fait tout ce qu'on dit, c'est-à-dire qu'elle intervient dans leurs communications, elle usurpe leur identité, elle se mêle dans un débat, elle lance des thèmes sur le net, elle est très sophistiquée dans son approche, comme d'ailleurs les Syriens commencent à le devenir. C'est-à-dire que donc on peut modifier par exemple l'agenda sur Facebook, des débats sur Facebook, comme ça, ce qu'ils font. Mais c'est un outil de police, de contrôle des dissidents. Dire que c'est un outil de guerre que dans la mesure… je ne parle pas des achats militaires, je comprends bien que par ailleurs ça peut devenir des outils de guerre. Enfin la police a des revolvers, c'est quand même une police, ce n'est pas un armée. Je veux dire évidemment quand on passe en situation révolutionnaire, les choses changent bien entendu, hein, on est bien d'accord là-dessus. Voilà, je dis ça parce que c'est important « arme de police », « arme de guerre », il faut y réfléchir parce qu'entre autres, ça a des conséquences sur les montages juridiques auxquels il faut avoir recours, et j'ai bien noté ce que vous disiez à la fin de votre intervention, c'est évidemment très important. Parce qu'on ne finira pas du tout, on est à un moment de très grandes opportunités sur ces questions, j'y reviendrai dans cinq minutes et selon qu'on va pousser dans une direction ou dans l'autre, on aura des avantages et des impasses. Il faut donc bien faire attention aux choix que nous lançons en ce moment, à mon avis.

La deuxième chose que je veux dire. En tous cas, qu'on soit dans une tyrannie comme avec Ben Ali, ou même dans un régime autoritaire comme le Qatar ou le Maroc, même si aujourd'hui le Maroc est en train de changer, ou disons le Maroc d'il y a trois ans ou cinq ans quand Amesys y travaillait, le cyberespace est un espace de confrontation c'est sûr. Entre un État, ses plates-formes et d'un autre côté des forces de changement. Alors avec une question qui vient tout de suite derrière, c'est, l'État a un deuxième recours derrière les systèmes d'inspection qui est « je coupe » ou « je ne coupe pas » Internet. Je vous l'ai dit tout à l'heure Ben Ali s'est posé la question de couper l'accès à Facebook, c'est-à-dire qu'il n'y avait plus du tout d'accès à Facebook en Tunisie. Compte tenu de toute façon qu'en Tunisie il était déjà impossible d'avoir accès à Flickr, à YouTube etc. Ce qui veut dire que les seuls échanges vidéo qui pouvaient se faire étaient par Facebook. Ce qui explique pourquoi Facebook a joué un rôle aussi important pendant le soulèvement, parce que c'était le seul moyen de faire circuler les vidéos des téléphones, hein, voilà. Sauf pour les gens qui avaient des proxys. Alors « on coupe » ou on « coupe pas »? Ben justement la Tunisie et la Libye qui s'était doté finalement à peu près à la même époque, et peut-être un peu avant pour la Libye finalement je découvre après, je pensais que la Tunisie – finalement- Ben Ali était premier, enfin ce n'est pas sûr maintenant, les Libyens eux ont beaucoup coupé Internet pendant la guerre civile hein, alors que finalement Ben Ali ne l'a pas fait.

Probablement, je pense, sous pression américaine, je pense que ça a été débattu, et je pense que l'ambassadeur tunisien a été convoqué à Washington, voilà, je pense que tout ça ne s'est pas fait. Il faut bien voir qu'il y a un jeu diplomatique géopolitique très compliqué dans la mesure où derrière le 11 septembre, les États-Unis au département d'État ont créé un bureau obscur en disant quand même créer un état d'esprit hostile à l'islamisme, et surtout l'islamisme radical. Et donc ils ont soutenu des blogueurs, ils ont aidé à se rencontrer, ils ont donné des formations, et comme ça tout un tas d'activités, hein, plusieurs blogueurs importants que j'ai interviewés en Tunisie, évidemment je ne donnerai pas leur nom, sont allés à des stages comme ça, financés directement par le département d'État ou en seconde main, ça dépend des stages, voilà. Je sais que ça a été le même cas en Égypte, bon, etc. Je dis ça pour dire que d'un côté la diplomatie américaine a renforcé avec l'arrivée de Clinton tout ça, il y a un type important qui est monté là-bas bon on parlera de tout ça plus tard peut-être, mais elle joue ça, autrement dit par rapport aux sociétés et aux intérêts commerciaux il y a évidemment des contradictions, et il y a du jeu dans le système américain. Le dernier truc qu'a fait Clinton à Amsterdam il y a quatre jours dont tu faisais écho c'est tout à fait dans ce cadre... De la « diplomatie digitale » comme on dit. D'ailleurs il est interdit aux entreprises américaines depuis 2004 d'exporter du matériel de ce type en Syrie. Dans la liste des trucs interdits en Syrie, il y a ça. Et toutes les sociétés qui ont collaboré l'ont fait en vendant à des entreprises européennes qui l'ont installé en Syrie ou en Libye, en tout cas en Syrie.

Je ne veux pas parler trop longtemps mais je voudrais encore dire une chose, c'est que, dans l'année 2011 il y a quand même, au moins, en Tunisie et en Libye, le soulèvement a gagné, et la surveillance de l'Internet ne se pose pas dans les mêmes termes. Est-ce que Internet joue aujourd'hui un rôle aussi important ? Je dirais il joue malgré tout un rôle moins important dans la mesure où sont apparus des médias libres. Parce qu'à l'origine quand même on surveille Internet là-bas pour surveiller les blogueurs. Tous ces gens qui donnent des mauvaises opinions, c'est eux qu'il faut identifier, pourchasser et faire taire, hein, ça sert à ça. Il y a qu'en Égypte où les réseaux militants se sont servis lors d'une grève en 2008 des médias numériques et où donc le gouvernement égyptien a décidé de surveiller les militants, mais ailleurs, c'est de l'expression qu'on veut interdire ce n'est pas des militants, hein on cherche l'expression. Or bien évidemment, dès lors que vous aviez des médias libres, plus vous avez des radios libres plus vous avez la TV libre, et bien moins effectivement les opinions qui sont données sur Internet ont de l'importance pour l'État en place, je ne parle pas pour les internautes.

Une autre question qu'il faut se poser aussi, c'est deuxièmement que sont devenus les systèmes de la tyrannie ? Parce que moi je ne sais toujours pas, on ne sait toujours pas combien il y avait de gens employés en Tunisie, des chiffres très divers circulent, entre 2000 et 6000, c'est évidemment pas la même chose. On ne sait pas où ils étaient logés, et ce qu'ils étaient à l'ATI [Agence Tunisienne d'Internet] ? Il y a beaucoup de gens qui

soutiennent qu'il y en avait plusieurs centaines qui travaillaient directement avec le palais de Carthage, alors moi ça m'a été affirmé à plusieurs reprises. Il y en a d'autres qui pensent, qui vous disent, qu'en fait au ministère de l'intérieur il y avait aussi dans la police un service qui travaillait directement sur Internet. Enfin on n'a même pas le diagramme organisationnel de qui avait accès à cette plate-forme et qui la manipulait juste derrière. Et on ne sait pas ce que sont devenus les gens. Je veux dire le système est-il encore techniquement opérationnel, supposons que demain ça tourne mal en Tunisie, pour n'importe quelle raison, est-ce que le système peut être remis en route ? Voyez c'est des questions qu'il faut se poser.

M. Jean-Marc Manach, journaliste. (53 min 14 s). Il y a des sites qui me semble-t-il ont été interdits après la fuite de Ben Ali.

M. Jean-Marc Salmon, chercheur. (53 min 20 s). Oui, bien sûr, mais je ne pense pas que ce soit du repérage avec ce système personnellement, mais je dis ça au feeling hein, je n'ai pas de preuve.

M. Christian Paul, député. (53 min 29 s). Est-ce que le contrat de maintenance court encore ?

M. Jean-Marc Salmon, chercheur. (53 min 20 s). Non, et alors voilà, une chose importante que j'ai appris techniquement par rapport à ce que disait Olivier, et à la DRM, en Libye, c'est que en Tunisie il y a une vingtaine d'étrangers qui sont venus et qui sont restés plus d'un an. C'est-à-dire que la mise en œuvre d'un système comme ça est compliqué, l'apprentissage est long. Voilà, c'est ça que j'ai compris, et j'ai eu le sentiment, dans la conversation, parce que les choses étaient pas dites, on ne vous donnait pas le nom de la société, de la même façon on ne disait pas ça, j'ai eu le sentiment que ça pouvait être des gens, des représentants d'un État, et non par les agents d'une entreprise privée, voilà. Je pense que vous posez des questions intéressantes, sur pourquoi est-ce qui y a eu des agents de la DRM et si c'est le cas pourquoi c'est eux qui ont fait la mise en œuvre bien sûr.

On va lancer le débat, je voudrais dire pour le débat vous avez compris un peu ce que j'en pense déjà. Premièrement je pense qu'il faut bien réfléchir à, est-ce qu'on dit que c'est une arme de guerre ou est-ce qu'on dit que c'est une arme de police où est-ce qu'on dit que c'est les deux? Est-ce qu'on veut une législation qui rentre dans le cadre des armes de guerre ou est-ce qu'on veut une législation spécifique? Il y a des choses qui vont dans le sens d'une législation spécifique, il y a des projets de législation, il y a des projets de loi aux États-Unis, ou de directives ici qui ont été déposées devant les parlements, qui traînent, qui si ces affaires-là prennent de la vigueur vont pouvoir être réactivées c'est une première chose, la Syrie est, deuxièmement, à mon avis quelque chose qu'il faut absolument utiliser. Je suis personnellement… Les gens de RSF m'avaient dit de travailler dessus, et donc j'avais commencé à regarder, on en avait parlé tout ça, moi quand je vois tout ce qui est déclaré à Bloomberg on ne sait pas si c'est du lard du cochon, on ne sait pas si [incompréhensible] vont sauver leur contrat ou s'ils ont décidé d'arrêter.

Intervenant non reconnu. (55 min 37 s). AREA…

M. Jean-Marc Manach, journaliste. (55 min 38 s). AREA c'est ça?

M. Jean-Marc Salmon, chercheur. (55 min 39). Oui…

M. Jean-Marc Manach, journaliste. (55 min 40 s). Oui, c'est une entreprise italienne qui avait envoyé des techniciens en Syrie, alors que la répression avait commencé, pour aider les services de renseignements syriens à surveiller la population syrienne.

M. Jean-Marc Salmon, chercheur. (55 min 50 s). Parce que ce qu'on lit quand même c'est que le matériel de Hewlett-Packard, qui est arrivé de Hewlett-Packard, est en Syrie. On le lit dans la dépêche.

M. Jean-Marc Manach, journaliste. (55 min 56 s). Ce qu'a dit Qosmos à Bloomberg ...

M. Jean-Marc Salmon, chercheur. (56 min 01 s). Ce n'est pas la même chose que le matériel de Qosmos hein, qui lui, passe par l'Allemagne...

M. Jean-Marc Manach, journaliste. (56 min 05 s). Ce que dit Qosmos à Bloomberg[62] est très intéressant. Quand les journalistes de Bloomberg demandent au PDG français de Qosmos, « vous avez du matériel en Syrie? » « Oui. On a décidé il y a trois semaines, de nous retirer de ce contrat, mais c'est techniquement et contractuellement compliqué ». Ils ont décidé au conseil d'administration de se retirer de la Syrie, mais ils ne savent pas comment faire.

M. Jean-Marc Salmon, chercheur. (56 min 24 s). Voilà c'est ce que je pensais, je suis bien content que vous ayez trouvé ça, parce que on voit bien, en fait, parce que si vous lisez les premières dépêches de presse, *quasiment rien n'est là-bas*, *rien n'est là-bas*, et finalement heureusement *on se méfie*, *on est en train de se retirer, c'est compliqué juridiquement mais on va*… Finalement ce qu'on comprend c'est que l'essentiel du matériel est là-bas, qu'en fait il y avait du monde là-bas, voilà, c'est ça qu'on comprend, alors il dit maintenant *j'en ai plus*. Bon d'accord sur le moment de l'interview, et puis qu'est-ce qui leur a pris, et qu'est-ce qui peut être sous-traité à l'étranger? Autre question bien entendu. Et donc moi, par rapport à ça, j'ai beaucoup poussé la FIDH qui est une organisation de droits de l'homme internationale, à monter au créneau sur la question de la Syrie[63], à demander des explications, alors c'est bien tombé parce qu'il y a 10 jours il y avait eu une réunion du forum droit de l'homme avec Ashton, notre ministre des affaires étrangères européennes à Bruxelles, voilà, et donc la présidente de la FIDH lui a dit mais alors la Syrie, machin, tout ça, franchement vous pensez pas qu'il est temps d'arrêter ces contrats, de faire un moratoire?

Donc ils sont très gênés, ils ont dit qu'ils allaient travailler, discuter, il y a à la fois un enjeu de court terme et un enjeu de moyen terme, de déboucher sur une législation. C'est une idée qui avance à Bruxelles, à gauche et à droite, voilà, parce que ça fait quand même extraordinairement désordre, et je pense que plus on arrive à en parler, évidemment c'est toujours plus compliqué qu'on imagine d'arriver à faire en sorte qu'on en parle, mais enfin quand même, plus on arrive à en faire une affaire publique, en France et dans les autres pays européens, plus on arrive à la monter, et plus je pense qu'on peut arriver à un cadre européen de contraintes sérieuses. Parce qu'entre autres le président du parlement européen est là-dessus lui aussi sur des positions, c'est un Polonais, il est sur des positions strictes. Il est de droite mais il est sur des positions strictes voilà, ce qui dans ce système bruxellois est important. Donc je pense qu'il faut demander un moratoire sur la Syrie, je pense qu'il faut demander un encadrement des ventes, et surtout des reventes, par des pays biais, et je pense que indépendamment d'une législation française, qui évidemment est toujours souhaitable, ça serait très bien d'avoir un deuxième verrou qui serait une législation européenne, qui de toute façon aurait le dessus sur la législation française.

M. Jean-Marc Manach, journaliste. (59 min 16 s). Si je peux juste me permettre deux points, dans l'interview que Amesys a donné à France 2, il y a un autre moment qui est très très intéressant c'est le moment où M. Samtmann montre un crayon à la caméra en disant : « mais voyez, moi j'ai vendu le crayon, je ne suis pas responsable de ce qui en a été fait ». C'est intéressant à deux titres, d'une part parce que les systèmes d'interception des télécommunications c'est pas des crayons, ce sont des armes qu'on ne vend que dans des salons d'armement. Enfin pour rencontrer Amesys, c'est soit Milipol soit ISS. ISS je peux pas y aller, je n'ai pas le droit de rentrer. Quand je pose des questions ils ne répondent pas aux questions, je suis allé voir à Milipol ils n'ont pas plus répondu aux questions mais en tout cas voilà ce sont des marchands d'armes. Par contre, effectivement, quand on regarde la liste des personnes dont on a les noms et les preuves qu'Amesys a permis leur espionnage, ce sont tous des journalistes ou des blogueurs. Ce sont tous des gens qui effectivement n'utilisaient pas un crayon mais un clavier pour s'informer et informer les autres,

---

62 Syria Crackdown Gets Italy Firm's Aid With U.S.-Europe Spy Gear : http://www.bloomberg.com/news/2011-11-03/syria-crackdown-gets-italy-firm-s-aid-with-u-s-europe-spy-gear.html
63 La FIDH et la LDH ont porté plainte contre X avec constitution de partie civile auprès du Tribunal de grande instance de Paris mettant en cause la société Amesys, filiale de Bull, pour complicité d'actes de torture en Libye : http://www.fidh.org/la-FIDH-et-la-LDH-deposent-une http://reflets.info/plainte-de-la-fidh-contre-amesys/

Intervenant non reconnu. (1 h 00 min 06 s). Et c'était des civils…

M. Jean-Marc Manach, journaliste. (1 h 00 min 07 s). Et c'était des civils. Mais des gens qui utilisent l'écriture pour arriver à informer les autres. Et j'ai mentionné tout à l'heure qu'il y avait un ambassadeur et un ministre, dans les deux autres grandes figures qui ont été espionnées, il y avait le responsable du principal forum de discussions des Libyens qui vivait en exil, et le responsable, le directeur de publication du principal média d'information libyen, également en exil.

Je voudrais revenir à un autre point sur ce que disait tout à l'heure Olivier concernant l'analogie avec le nucléaire, je pense que l'analogie elle tient également en matière de prolifération. C'est-à-dire que là on a une entreprise privée, qui, avec l'accord de l'État français, un accord tacite à défaut d'un accord écrit, a vendu à un dictateur du matériel d'interception des télécommunications dont on pouvait supposer qu'il allait servir à réprimer une population civile, mais qui ne s'est pas contentée de ça, en plus il a apporté là-bas un soutien technique en envoyant des Français, c'est marqué dans la proposition de contrat : « Nous allons envoyer deux ingénieurs français pendant six mois » et dans les faits ils y allaient beaucoup plus souvent que ça, le ou les ingénieurs français, bon, je veux pas rentrer dans les détails, mais enfin on sait qu'il y a une assistance qui a été faite, et l'article du Wall Street Journal aujourd'hui[64] révèle que le nom du chef de projet d'Amesys un Français, un jeune Français, était affiché dans les locaux du centre d'interception avec son adresse e-mail et son numéro de téléphone, *si vous avez un problème technique, n'hésitez pas à le contacter*. Et en réponse quand on demande *mais comment ça se fait qu'une liste de dissidents libyens figure dans le mode d'emploi d'Eagle ?* La réponse de M. Samtmann c'est de dire : « C'est le client qui nous a fourni la liste ». Donc c'est assez étonnant de voir qu'un client aide un producteur, un fabricant à créer un mode d'emploi, mais en tout cas on voit bien que le producteur et le client ont travaillé de concert et que le producteur ne pouvait pas ne pas savoir.

Voilà, donc il y a eu une assistance, donc je pense que pour réfléchir à cette notion de moratoire ou d'embargo ou comment on va réguler et encadrer cette chose-là, il faut poser aussi cette chose-là aussi sous l'angle de la prolifération, mais comme on parle de non-prolifération nucléaire, à savoir que là si on fait l'analogie avec le nucléaire, non seulement ils ont vendu de quoi faire une centrale nucléaire, mais en même temps ils ont envoyé là-bas des techniciens pour aider à fabriquer la centrale et à la faire tourner. Donc ça c'est le premier point et le deuxième point sur la non-prolifération c'est aussi ce qu'a répondu Bluecoat qui a dit nous n'avons rien vendu à la Libye nous avons vendu à -je sais plus- si c'est un qatari qui lui-même l'a vendu à la Syrie. Comment on fait pour faire de telle sorte qu'on ne puisse utiliser des faux-nez, pour que ce genre de système puisse se retrouver dans un pays où ça va servir à réprimer les civils.

M. Olivier Laurelli, cofondateur Reflets.info. (1 h 02 min 41 s). Si je peux me permettre pour rebondir là-dessus, il y a quelque chose qui est très intéressant, c'est la différence de réaction des entreprises françaises et américaines. Au début les entreprises nient. Ce qui s'est passé aux États-Unis, c'est que le département d'État qui s'est très, très vite intéressé à l'affaire, a mis un petit peu la pression sur Bluecoat, et Bluecoat a été finalement condamné à 1 million de dollars d'amende, ce qui est « Peanuts » par rapport à leur chiffre d'affaires évidemment. Il faut savoir que l'affaire a explosé c'était fin juillet début août où on a commencé à parler de ses « appliances » en Syrie, ça a été réglé au mois d'octobre, Bluecoat a été condamné à une amende. Amesys, cette affaire était révélée au mois de mai dernier, voilà, même février, on a commencé à en parler en février dernier, les premières questions au gouvernement sont arrivées au mois d'août, fin août, aujourd'hui on est en décembre, il y a pas une seule réponse aux questions qui ont été posées au gouvernement. Il n'y a pas l'ombre d'un soupçon de sanction possible encore sur ces entreprises.

M. Jean-Marc Salmon, chercheur. (1 h 03 min 53 s). Pour réagir par rapport à ce que vient de dire Jean-Marc, une piste possible parce que la question de la prolifération est une question évidemment cruciale dans cette affaire, je suis bien d'accord j'aime bien ce mot de prolifération. Une piste possible pour en limiter les dégâts ce

64 Life Under the Gaze of Gadhafi's Spies : http://online.wsj.com/article/SB10001424052970203764804577056230832805896.html

serait de reprendre l'idée de reporters sans frontières qui serait finalement de modifier la législation internationale et en tout cas européenne pour que les organisations de droits de l'homme puissent attaquer en justice les sociétés s'il se révèle que ce qu'elles ont vendu a servi à réprimer des gens. Et du coup la question de j'ai vendu un machin mais je ne savais pas etc. il faudra le démontrer, ce qui est un petit peu plus compliqué que de le dire.

M. Christian Paul, député. (1 h 04 min 48 s). Simplement juste un point en écho à ce que disait Jean-Marc Manach tout à l'heure, on voit bien qu'on est devant des technologies duales, ça a été dit, à la fois possiblement armes de guerre et outils de police, et probablement selon les moments et selon les utilisateurs l'un ou l'autre. Si on ne relève pas d'armes au sens matériel de guerre effectivement on échappe à la commission, c'est pas parce qu'on échappe à la commission qu'il n'y a pas un accord explicite et un feu vert politique ça veut dire que, apparemment, on verra ça si on a enfin un jour une réponse du gouvernement d'aujourd'hui, il y a eu contournement de la commission ou il y avait pas besoin de passer devant la commission, ça veut pas dire qu'il n'y a pas eu un feu vert politique. Moi je serais extrêmement surpris que, en direction de la Libye et de la Syrie notamment -bon le Maroc, la Tunisie c'est peut-être un peu différent- je serais très surpris qu'il n'y ait pas, je n'imagine pas un instant, dans la façon dont fonctionne l'appareil d'État sur ces questions, entre le ministère de la défense, le cabinet du premier ministre et la présidence de la république, j'imagine pas un instant qu'il n'y ait pas un feu vert explicite au plus haut sommet de l'État quand il s'agit de mettre entre les mains d'un régime, certes nouvellement ami, mais enfin, quand même considéré assez généralement comme un régime autoritaire, voire une dictature, je crois qu'il y a eu feu vert politique. Bon une commission d'enquête permettrait...

M. Jean-Marc Manach, journaliste. (1 h 06 min 25 s). Clairement Philippe Vannier a déclaré[65] en 2009 que le contexte réglementaire français était tellement complexe, qu'il fallait de toute façon avoir une validation de la part des autorités, et que des pays étrangers en profitaient pour remporter des marchés que la France n'arrivait pas à remporter tellement c'était compliqué de travailler avec certains pays, et il prononçait pas le nom du pays, mais on comprenait très bien que c'était ces pays qui n'étaient pas clairement des démocraties. Donc il l'avait dit bien avant le scandale Amesys donc c'est évident qu'il y a un contrôle qui est fait de la part de l'exécutif et de gens au sein du ministère de la défense avant de faire quelque affaire que ce soit avec ce genre de pays.

M. Olivier Laurelli, cofondateur Reflets.info. (1 h 06 min 58 s). Enfin il faut savoir que les entreprises en plus ont d'autres leviers, si vous prenez le cas d'Alcatel qui opère la censure en Birmanie par exemple, elle le fait par le biais d'une filiale qui s'appelle Alcatel Shanghai Bell[66] qui officiellement n'a aucun point d'attache en Birmanie, mais qui occupe le cinquième étage d'un hôtel de luxe là-bas.

M. Christian Paul, député. (1 h 07 min 17 s). Alors je vous propose qu'on fasse, qu'on prenne des interventions qui peuvent être d'ailleurs des questions aux intervenants ou des témoignages ou des prises de position évidemment, simplement j'indique que nous avons un enregistrement donc si vous souhaitiez pas figurer dans l'enregistrement, vous nous le dites et on le coupe, ce que je demande également à chacun c'est par souci de transparence des débats de se présenter bien sûr avant d'entamer son intervention.

M. Bruno Carrias, consultant. (1 h 07 min 49 s). Oui, Bruno Carrias, je suis consultant et je suis intervenu entre autres sur la commission « Bravo » [du nom du président de cette commission, Alain Bravo, membre de l'Académie des technologies, directeur général de Supélec] sur la prospective économie numérique 2025[67] et j'étais en charge plutôt des aspects plutôt libertés publiques, citoyens, tout ce qui était dispositifs démocratiques. Je trouve que cette initiative, Monsieur le député, est excellente, puisque vous êtes complètement dans la logique de vous interroger sur des risques qui peuvent apparaître sur le contrôle ou sur

65 Amesys, la Libye, Nicolas Sarkozy, et la minute nécessaire de monsieur Cyclopède : http://reflets.info/amesys-la-libye-nicolas-sarkozy-et-la-minute-necessaire-de-monsieur-cyclopede/
66 Alcatel Shanghai Bell et Deep Packet Inspection en Birmanie : http://reflets.info/alcatel-shanghai-bell-et-deep-packet-inspection-en-birmanie/deep-packet-inspection-en-birmanie/
67 La société et l'économie à l'aune de la révolution numérique Enjeux et perspectives des prochaines décennies (2015-2025) :
http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics//094000332/0000.pdf

l'utilisation de techniques numériques si vous voulez, vis-à-vis d'expression, vis-à-vis de la création de rumeur, vis-à-vis d'éléments de déstabilisation parce ça va au-delà simplement du contrôle des personnes, des écoutes, et on voilà bien aujourd'hui la puissance qu'il peut y avoir autour d'un outil très séduisant comme Internet par exemple, mais y a pas qu'Internet, d'ailleurs, il y a le téléphone, il y a plein d'autres choses qui sont autour, mais en même temps des risques qui sont associés. Pour autant je ne vous rejoins pas si vous voulez sur la manière dont vous faites cette analyse, parce que je pense qu'elle est prise peut-être d'une manière trop restrictive. Non pas que ce que vous avez évoqué soit contestable, vous évoquez un certain nombre de points que je ne remets pas en cause, mais sur la manière de l'analyser.

Alors premier point, vous avez parlé effectivement armes de guerre, armes de police. Le problème c'est que les technologies qui sont utilisées ne sont pas toujours « *packagées* » sous forme de système. Ce sont des matériels, ce sont des systèmes, ce sont des technologies qui sont à la fois duales pas simplement parce qu'elles sont civiles et militaires, mais parce qu'elles font partie même de l'administration de ces réseaux. Et donc vous avez d'entrée, et d'ailleurs c'est vous même qui l'avez signalé, la technique DPI ou tout ce qu'il y a autour parce qu'il n'y a pas simplement que cette technique qui peut être utilisée pour, à la fois, de la régulation et du contrôle, sont à la fois indispensables, ne serait-ce que sur le plan technique si vous voulez, pour pouvoir gérer ces dispositifs, elles sont probablement cruciales pour faire que Internet ne soit pas un lieu de non-droit dans lequel, toutes les mafias du monde se déverseraient -ce qui est déjà le cas, dans lequel toutes les perversions aussi pourraient se déverser sans qu'il puisse y avoir certains contrôles, et on voit bien qu'on a une vraie difficulté. Alors vous signalez des points qui sont peut-être condamnables, qui sont peut-être à la marge, là-dessus il faut qu'il y ait débat, ça pose une vraie question mais ça n'est qu'une partie de la réalité puisque la menace sur Internet est infiniment plus importante si vous voulez que celle que vous développez aujourd'hui, qui est un cas important certes mais qui est sur des contextes très particuliers : révolutions arabes, systèmes relativement totalitaires. Or aujourd'hui même dans une démocratie on a une vraie problématique dans ce domaine-là. Ce qui rend d'ailleurs les difficultés sur, si vous voulez, sur le fait de légiférer, puisqu'on voit bien toute la difficulté sur la notion de « comment légiférer ».

Deuxième dispositif, c'est dès qu'on légifère, c'est le domaine d'application, et vous avez bien indiqué en prenant l'exemple du routage qu'on est dans un environnement globalisé. Je ne sais pas aujourd'hui séparer, pas plus que le nuage de Tchernobyl, dire que les frontières séparent les flux Internet, et quand vous communiquez de l'un à l'autre, parce que j'en ai vu tout à l'heure qui twittaient ou chattaient ou peu importe, vous ne savez pas du tout par où ça passe. Et ça passe par des centres qui sont hors de la souveraineté, qui soit souveraineté européenne, souveraineté nationale ou autre, avec toutes les difficultés qu'il peut y avoir pour qualifier les faits, mais en même temps pour poursuivre les intervenants, et même pour les intervenants qui sont on va dire relativement rustiques. Parce que dans ce domaine là dès qu'on parle information vous avez des combinaisons extraordinaires dans lesquelles des institutions, des états, et tous les états, après c'est un problème de moyens, tous les états interviennent avec des faux-nez. La discussion par exemple sur le fait de déclarer de la part du département d'État américain que la solution qui serait une solution française est condamnable, ou que ces techniques sont condamnables, dans le même temps si vous voulez l'administration américaine utilise des multiples moyens dont Facebook le premier, parce que j'ai lu quelque part probablement sur votre site qu'il était préférable d'avoir un rapport commercial avec Facebook ou avec Google, que nenni. Facebook et Google sont une vraie problématique d'impérialisme probable, que l'on peut avoir dans le domaine de la manipulation des systèmes d'information. Des systèmes d'informations, certes qui sont moins rustiques que peut-être le cas que vous avez signalé, mais qui sont infiniment plus dangereux.

Derrière ça touche pas seulement le cas de la communication, on parle de plus en plus aujourd'hui du problème de l'authentification des personnes, de la relation qu'il peut y avoir entre les multiples liens, comportements, actes si vous voulez qu'ils peuvent faire. L'authentification aujourd'hui est en train de se diriger si personne n'intervient, sur probablement trois ou quatre acteurs mondiaux. On aura deux chinois - puisqu'en général ils vont par deux, il y a deux acteurs s'il y a deux sites avec toujours systématiquement deux

technologies différentes, s'il y a trois technologies il y aura trois acteurs chinois- il y aura probablement deux ou trois acteurs américains dont on connaît déjà les noms -il y a probablement Apple et probablement Google. Et puis après il y a un véritable enjeu qui est aussi un enjeu à notre niveau, que ce soit l'Europe, en particulier, voire peut-être d'autres pays émergents dans lesquels ces technologies doivent pouvoir être utilisées. Donc le problème ne semble pas de coller au pilori des sociétés. Si les sociétés en cause ont commis des actes délictueux, qu'elles soient sanctionnées. S'il y a quelques points sur lesquels on peut effectivement corriger quelques trous béants, disons, dans une réglementation, législation qui a toujours un peu du mal à suivre l'exercice –et là ce n'est pas un reproche Monsieur le député- a toujours des difficultés à suivre l'exercice civil. Mais il ne faut pas être tout à fait naïf, on a depuis la nuit des temps des cabinets noirs, des cabinets obscurs si vous voulez qui existent, des officines. La différence si vous voulez c'est que ces outils sont infiniment plus puissants et que quelque part les victimes sont presque des victimes consentantes, puisqu'elles utilisent à fond pour une large part, je ne parle pas des personnes de la révolution arabe, les trois quarts des personnes livrent aujourd'hui sur leur vie privée des informations qu'elles n'auraient jamais livrées à une enquête quelconque de police. Quand je vois par exemple, la réaction qu'il a pu y avoir sur certains fichiers centralisés et qui étaient pourtant couverts par des instances dans un cadre légal, comme par exemple les écoutes, et qu'on voit aujourd'hui ce qu'on peut mettre sans aucun contrôle des données, sans aucune possibilité de le changer, avec une impossibilité même de savoir s'il n'y a pas eu une modification de votre propre authentification sur le réseau, là on a de vraies questions à se poser. Je pense sur ce plan-là, qu'il y a peut-être de manière accessoire quelques questions que vous avez posées mais je pense que cela ne traite pas le problème de fond qui est infiniment plus complexe, je pense que au-delà des aspects périphériques qui peuvent être aussi liés à l'actualité ou qui peuvent être des problèmes de responsabilité politique, ...

[Le public demande à ce que la table ronde soit respectée avec un changement d'orateur, celui qui parle depuis 10 minutes se défend].

M. Bruno Carrias, consultant. (1 h 15 min 08 s). Mais attendez, c'est un sujet de fond, la table ronde c'est un débat. On a eu pendant trois quarts d'heure un point de vue... mais je ne fais pas une erreur par minute, monsieur. Je me permets d'exprimer une position, une analyse, et jusqu'à maintenant...

M. Jean-Marc Manach, journaliste. (1 h 15 min 30 s). Je peux lui répondre en une minute ou pas ? On fait d'abord tourner ?

M. Christian Paul, député. (1 h 15 min 32 s). Oui on fait tourner.

M. Bruno Carrias, consultant. (1 h 15 min 34 s). Je ne critique pas ce que vous avez dit, je dis simplement que c'est un point de vue complémentaire.

M. Christian Paul, député. (1 h 15 min 38 s). J'entends un point de vue différent, et je répondrai éventuellement en conclusion tout à l'heure.

M. Bruno Carrias, consultant. (1 h 15 min 39 s). Bien sûr.

M. Christian Paul, député. (1 h 15 min 42 s). D'autres… ? Oui madame… Si vous pouviez éteindre le micro précédent, merci (s'adressant à M. Bruno Carrias).

M. Bruno Carrias, consultant. (1 h 15 min 46 s). Oui.

M. Christian Paul, député. (1 h 15 min 50 s). Chacun se présente…

Mme X, avocat. (1 h 15 min 52 s). Oui, bonsoir je suis avocat et je me spécialise en droit pénal de l'informatique donc je ne suis pas informaticienne. [Aléas avec le micro]. J'ai une pratique pénale. Je trouve que c'est très intéressant mais j'ai une question, qui est peut-être un petit peu bête, je ne sais pas, cette commission d'enquête, qu'est-ce que ça va vraiment changer concrètement ? Enfin, si j'ai bien compris, vous souhaiteriez

que le matériel de guerre, enfin que ce dont vous parliez soit intégré aux matériels de guerre. Mais en pratique, concrètement, est-ce que ça va être vraiment efficace ? Donc ça c'est ma première question.

La deuxième c'est plus des remarques. Je ne me permettrais pas de critiquer parce que, enfin, même si, si, finalement, je vais un peu critiquer, c'est qu'en matière d'écoutes téléphoniques, déjà c'est facile à annuler. Ce n'est pas compliqué à annuler, tant mieux pour tout le monde… [Commentaire inaudible en fond] Quand on est avocat dans le cadre d'une procédure pénale, d'accord ? [Commentaire inaudible en fond] Mais c'est vrai.

M. Olivier Laurelli, cofondateur Reflets.info. (1 h 17 min 07 s). Excusez-moi mais ça fait deux fois de suite avec deux intervenants différents, qu'on fait le comparatif avec des écoutes téléphoniques qui sont des écoutes ciblées par définition, là on parle de système d'interception à l'échelle d'une nation. Des systèmes d'interception globale.

Mme X, avocat. (1 h 17 min 18 s). Oui oui bien sûr j'ai bien compris… [Commentaire inaudible en fond]. Excusez-moi monsieur, c'est moi qui parle. Non, mais simplement le code de procédure pénale est pas toujours très bien rédigé, notamment la « Loppsi 2[68] », il y a des articles qui sont complètement hallucinants, mais qui peuvent pour moi parfois être utiles, parce que justement dans la mesure où c'est très mal rédigé, voilà il y a l'article 100[69] du code de procédure pénale, là il y a un article qui est plus récent mais en réalité on pouvait déjà, enfin... Il y a la notion de données informatiques, donc déjà avant peut-être de se poser des questions sur le matériel de guerre peut-être qu'il faudrait d'abord commencer par un peu plus clarifier... voilà. Et puis après évidemment bien mesurer que les organisations criminelles sans aller jusqu'à... utilisent nos téléphones, enfin vous devez le savoir mieux que moi pour se laisser des messages, c'est vrai qu'il y a aussi un besoin de prévention à l'attention des utilisateurs, et il y a un manque, et moi j'ai des dossiers de piratage téléphonique, où je suis pour des victimes, des sociétés qui ont été victimes, et qui ne sont pas négligentes, c'est qu'avec les... Il y a d'autres problèmes, si vous voulez, autour de ça, qui moi, je pense, il serait urgent qu'ils soient un peu plus réglés, il y a des législations là qui sont des obligations de notification des failles de sécurité on avance, mais encore faut-il que la CNIL, enfin moi là j'élargi le débat mais il y a des vrais problèmes, il y a des vraies contradictions et donc c'est vrai qu'il faut enfin moi j'ai cette idée à cœur, je pense qu'il faut interroger les hackers avant de faire une loi.

M. Christian Paul, député. (1 h 19 min 14 s). Je ne cache pas qu'il y en a quelques-uns et de bonne qualité autour de la table. Juste un mot et je vous donne la parole, qui est un peu en écho aux deux interventions précédentes, il est évident qu'on n'a pas choisi aujourd'hui d'évoquer toutes les questions qui relèvent de la régulation de l'Internet, ou toutes les questions qui relèvent du droit de l'Internet. L'objectif de cette table ronde, c'est de voir quels pouvaient être les réponses ou les ripostes à des atteintes très fortes aux libertés démocratiques qui ont été favorisées par l'usage des technologies de surveillance de l'Internet, voilà, on n'a pas un propos global sur la société de surveillance dans toutes ses formes.

M. Olivier Laurelli, cofondateur Reflets.info. (1 h 19 min 53 s). Une petite précision quand même parce qu'on me parle souvent d'Echelon pour comparer *Deep Packet Inspection* à Echelon, il faut arrêter avec ça. Si vous voulez, Echelon c'est un système qui réagit sur une base de dictionnaires, les systèmes qui sont vendus par Amesys sont des systèmes qui écoutent le contenu de l'intégralité des communications avec des « plug-ins » dédiés, qui stockent ces communications dans une base de données et qui propose une interface pour accéder aux communications globales de toute la population. [Commentaire inaudible en fond] Quand une entreprise comme Amesys vend au Maroc 4000 disques durs d'un téraoctet vous vous doutez bien que ce n'est pas pour écouter une fraction des connexions.

---

68 Loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure : http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000023707312&dateTexte=

69 Code de procédure pénale, Article 100 : http://legifrance.gouv.fr/affichCodeArticle.do;jsessionid=F672E9A533E60929056AE3802C2AB27D.tpdjo07v_2?idArticle=LEGIARTI000006575246&cidTexte=LEGITEXT000006071154&categorieLien=id&dateTexte=20111228

M. Bruno Carrias, consultant. (1 h 20 min 42 s). Oui mais attendez, vous avez des fermes aujourd'hui avec des...moi je comprends bien là-dessus, mais j'indique simplement que ces dispositifs, et quand on a parlé à un moment de, comment ça s'appelle, comme le nucléaire,... je trouve plus le mot, de prolifération, la difficulté qu'on a c'est que ces technologies sont utilisables avec des moyens qui sont relativement entre guillemets faibles, c'est-à-dire qui ne sont même plus du niveau de l'État, nous sommes d'accord sur ce point-là, alors que heureusement jusqu'à maintenant la prolifération nucléaire nécessite quand même un peu de moyens, je parle pas de la salle et des bombes qui sont évidemment un vrai problème, mais on voit bien quand même que la mise au point d'une filière est relativement longue, permet un certain nombre de contrôles des réactions qui sont plus faciles. Là, la difficulté qu'on a et je vous rejoins tout à fait, on a un vrai problème, parce que ces technologies sont à la portée de techniciens, simplement de bon niveau et de moyens relativement limités. Derrière, après c'est simplement un problème d'échelle, d'échelle et le nombre de personnes.

M. Olivier Laurelli, cofondateur Reflets.info. (1 h 21 min 47 s). Non, pour moi le problème est beaucoup plus conceptuel... [Petit flottement, M. Christian Paul règle le souci de prolifération de micros en rappelant que trois sont restés allumés].

M. Antoine Champagne, cofondateur Reflets.info. (1 h 21 min 58 s). Je pense que je vais être assez d'accord avec le monsieur qui est là puisque que je suis cofondateur avec lui du site Reflets, je voudrais juste rebondir sur deux choses. La première c'est sur le côté juridique législatif, comment faire pour essayer d'encadrer tout ça ? Moi j'ai un avis qui est le mien, qui est probablement pas partagé, mais il existe déjà une législation là-dessus. Pourquoi ? Je vais rebondir sur ce que disait Olivier, ce sont des outils qui servent à écouter les communications privées, donc il y a des textes là-dessus qui disent que effectivement c'est interdit, ou en tout cas si on veut le posséder, le construire ou le vendre, on doit passer devant une commission pour obtenir un accord du premier ministre. Après une fois que l'accord est donné, effectivement c'est légal. [Commentaire inaudible en fond] Non, je ne parle pas que de la France et je m'adresse aux juristes que vous êtes par nature, quand, comme la loi dit « vendre », pour moi « vendre » c'est une conception juridique large qui couvre les exportations, à partir du moment où j'exporte, j'ai vendu. Donc si je vends, je tombe sous cet article 226[70] dont on parle depuis tout à l'heure. C'est mon analyse de la chose, j'ai vraiment regardé tous les textes qui étaient liés à cet article…

M. Jean-Marc Manach, journaliste. (1 h 23 min 23 s). C'est pas l'analyse de l'ANSSI, c'est pas l'analyse de Matignon, ni du gouvernement…

M. Antoine Champagne, cofondateur Reflets.info. (1 h 23 min 28 s). Oui c'est ce que j'ai dit en préambule, c'est mon analyse, peu m'importe en fait l'analyse de l'ANSSI je dois dire. Je pense qu'ils sont tout à fait d'accord avec le gouvernement puisque c'est une décision totalement politique et que la décision politique -comme on l'a tous dit ici- a été donnée de vendre à la Libye, pour Qosmos probablement d'aller vendre ses sondes à la Syrie en plein massacre. Et on a évoqué vaguement jusque-là, et je vais revenir là-dessus, ce que je voulais dire, c'est que aujourd'hui, vous disiez Madame qu'est-ce qui va changer avec la commission d'enquête ? A mon avis pas grand-chose, je vais vous dire pourquoi. Parce qu'Amesys a des dizaines et des dizaines de contrats encore aujourd'hui en cours avec tout ce qui est le cœur de la défense française, avec des Thales, avec des Eurocopter, la DGA[71], etc. Des documents qui montrent ça j'en ai une pile à peu près haute comme ça. Je sais qu'ils sont actuellement en train de faire ce commerce, pour d'autres choses, donc effectivement ces gens-là vont continuer à vendre sans souci et ils auront toujours des liens politiques et industriels qui feront qu'ils pourront continuer à faire ça.

Et je vais juste terminer là-dessus, on n'en parle pas mais le mois dernier -Olivier a évoqué le sujet- le mois dernier, Amesys a payé deux millions de dollars pour pouvoir acheter le matériel nécessaire pour installer le

70 CF note 34.
71 Amesys : le lourd poids du secteur militaro-industriel : http://reflets.info/amesys-le-lourd-poids-du-secteur-militaro-industriel/

même système au Maroc[72], ça va être livré là, aujourd'hui. Je veux dire le gouvernement français se contrefout de ce que tout le monde, tous les journalistes disent, et donne probablement un nouvel accord pour que ce matériel soit exporté, sorti de France, puisque c'est livré. Alors c'est du matériel américain, c'est IBM, mais c'est livré par une filiale de Bull, Serviware. On l'a écrit, c'est dans Reflets, c'est dans le Canard enchaîné, pff… Voilà. Tout ça part dans les limbes. Aujourd'hui Amesys se fait payer quatre cents mille dollars par une société qui fait du « *Homeland Security* » aux Emirats Arabes Unis, on se doute que ce n'est pas pour vendre, je ne sais pas moi, on comprend bien pourquoi.

M. Christian Paul, député. (1 h 25 min 57 s). Vous en concluez quoi ?

M. Antoine Champagne, cofondateur Reflets.info. (1 h 25 min 59 s). J'en conclus que ça va continuer, qu'il n'y a aucun moyen d'arrêter ça.

M. Christian Paul, député. (1 h 26 min 02 s). Est-ce que c'est l'impuissance générale ?

M. Antoine Champagne, cofondateur Reflets.info. (1 h 26 min 04 s). Oui c'est l'impuissance générale. Juste pour finir effectivement aux États-Unis il s'est passé quelque chose, c'est pas transcendant mais il s'est passé quelque chose. Aujourd'hui ici en France, il ne se passe rien et pourtant on revient tous les trois jours sur ce sujet, que ce soit OWNI, que ce soit le Wall Street Journal, que ce soit Reflet, que ce soit le Canard enchaîné, [Commentaire inaudible en fond] même France 2, France 3 et TF1.

M. Christian Paul, député. (1 h 26 min 31 s). Bien qui souhaite compléter, intervenir, réagir ? Tout le monde est tétanisé par la dernière intervention ? Non ? Alors, allez-y…

M. X, informaticien. (1 h 26 min 44 s). Donc moi je travaille dans un service informatique d'une entreprise, est-ce qu'on peut juste, et je veux le demander à Olivier, est-ce qu'on peut juste revenir sur l'indispensabilité du DPI ? Juste pour bien clarifier les choses, parce que tout à l'heure face à l'intervention de monsieur [M. Bruno Carrias] en face, l'indispensabilité du DPI est-elle toute relative ?

M. Olivier Laurelli, cofondateur Reflets.info. (1 h 27 min 01 s). Alors, c'est plus que relatif, parce que les réseaux ont toujours fonctionné avant que ça existe de manière très, très bien, autonome et tout ça. Aujourd'hui les problèmes en matière de sécurité qui sont souvent argués sont l'une des principales raisons de l'usage du DPI. Le deuxième usage qui en est massivement fait c'est celui de la publicité donc que là j'ai tendance à vous dire que c'est pas du tout utile, il y a des gens qui vont dire non, non, c'est ça qui finance Internet, ce qui est totalement faux, c'est votre abonnement qui finance Internet. Il faut savoir que le DPI est sourd, muet et aveugle à partir du moment où vous chiffrez vos communications. Donc en matière de sécurité vu le type d'attaques qu'on voit aujourd'hui passer, des attaques très élaborées comme Stuxnet ou Aurora, et bien là votre sonde DPI elle sert à rien du tout, parce que le DPI par définition ça va reconnaître des protocoles qui sont déjà inscrits et qui existent, ça va pouvoir reconnaître certains algorithmes de chiffrement sans pouvoir lire la charge utile justement de la communication, donc il y a plein de moyens de neutraliser le DPI.

Là où c'est utile aujourd'hui c'est vraiment pour la surveillance de masse, je vous renvoie par exemple au papier[73] qui a été fait à Prague, à l'ISS de Prague en 2008 par Amesys, qui défend cette idée d'interception globale, que c'est mieux que faire de l'écoute légale parce que là au moins on a justement l'ensemble des communications, c'est-à-dire qu'on part du principe, du postulat, que tout le monde est un terroriste, un pédophile, un criminel. Donc il y a pas de choses indispensables à partir du moment où il y a, même pour aller chercher les gros méchants, un travail sur le terrain qui est fait, où il y a des écoutes ciblées, où l'on sait que c'est pas en écoutant l'ensemble d'une population, c'est pas en écoutant l'ensemble des communications qu'on n'arrive à prévenir un attentat comme le 11 septembre par exemple, moi j'ai tendance à dire qu'à force d'écouter tout le monde on finit par plus entendre personne. A partir de ce moment-là on peut se poser la

72 Amesys : un Finger de Pop Corn pour le Croco : http://reflets.info/amesys-un-finger-de-pop-corn-pour-le-croco/
73 Présentation Amesys ISS Prague 2008 : http://wikileaks.org/spyfiles/files/0/21_200810-ISS-PRG-AMESYS.pdf

question effectivement si c''est indispensable. Là où on va le retrouver de manière un peu plus utile et même si j'aime pas cette utilisation c'est dans la facturation et le bridage des réseaux 3G. Mais la typologie des réseaux aujourd'hui fait que si on exploite des ressources qui sont rares, et pour exploiter des ressources qui sont rares eh bien on a besoin d'outils de contrôle et de facturation. Là il faut avouer que le DPI est une technologie qui est tout à fait utile. Dans le cadre ensuite d'interceptions légales, là encore une fois pour intercepter du trafic non chiffré, c'est tout à fait utile. Effectivement que la gendarmerie possède un GLINT et fasse de l'écoute ça va pas me gêner plus que ça. Ce qui va me choquer beaucoup plus c'est que des officines aient accès à ce genre de technologie, mais là je vais être un petit peu alarmiste, il ne faut pas se leurrer, vous prenez la carte des câbles sous-marins, vous regardez, il y en a pas des masses, et vous pouvez être sûrs qu'ils sont tous sous surveillance. Tout le trafic qui passe dans ces câbles sous-marins est « *dumpé* ». La France comme les États-Unis ont une force de projection navale qui permet l'interception de signaux dans les fibres sous-marines. Voilà, partant de ce postulat on peut se demander si c'est réellement utile pour tout et n'importe quoi ? Non ce n'est certes pas utile et indispensable pour tout et n'importe quoi, mais il y a quand même certaines applications dans lesquelles cela peut être fortement utile.

M. Christian Paul, député. (1 h 30 min 25 s). Bien merci, alors ce que je propose c'est qu'on aille peut-être jusqu'à 20h30, c'est un peu le calibre qu'on s'était donné pour cette table ronde. Je laisserais bien sûr s'ils le souhaitent aux deux Jean-Marc qui m'entourent et bien sûr à Olivier la possibilité de réagir in fine, mais d'abord est-ce qu'il y a d'autres prises de parole, notamment parmi ceux qui n'ont pas encore pris la parole ? Oui ? Micro, présentation.

M. Emmanuel Aguet, informaticien. (1 h 30 min 52 s). Bonjour, Emmanuel Aguet, informaticien. Je souhaite réagir sur quelque chose, c'est qu'on a parlé du DPI, on n'a pas évoqué entre guillemets d'autres technologies où ce ne serait plus tellement le logiciel qui ferait le travail mais plus le matériel, c'est-à-dire, concrètement, du trafic chiffré peut être -au moins en théorie- déchiffré à la volée avec les bonnes clés, etc. Je ne rentre pas trop dans les détails… [Commentaire inaudible en fond] Oui, oui, volontairement. En gros enfin je trouvais étonnant qu'on n'en ait pas parlé en fait, parce que concrètement... [Commentaire inaudible en fond]

M. Olivier Tesquet, journaliste. (1 h 31 min 51 s). Bonjour Olivier Tesquet, je suis journaliste à Télérama, j'ai travaillé sur le sujet avec Jean-Marc il y a quelques mois. Je voudrais juste rebondir sur ce que disait Olivier, notamment sur l'utilisation du DPI. J'ai l'impression que la légitimation aujourd'hui elle est avant tout économique, c'est-à-dire que la raison de l'investissement du FSI dans Qosmos et dans Bull est probablement à chercher de ce côté-là. Je me souviens quand on en discutait au printemps avec Olivier, il me disait, en France on exporte quatre choses : « on exporte du bon vin, de la bonne bouffe, des droits de l'homme, et du DPI ». On a un vrai savoir-faire en la matière, et on se rend bien compte aujourd'hui que c'est quelque chose qui peut permettre de dégager des points de croissance. Quand il y a le rapport McKinsey[74] sur l'économie numérique qui sort, et dont le gouvernement fait ses gorges chaudes encore aujourd'hui, on se rend compte que parmi les dix exemples qui sont pris, dedans, on trouve Qosmos qui a une croissance qui est absolument exponentielle. Donc je pense que c'est un moyen aussi de légitimer cette utilisation là et c'est probablement une des raisons pour lesquelles le gouvernement a très longtemps fermé les yeux ou donné son aval sur ces choses-là, et je voudrais juste ajouter une toute petite chose c'est que j'en discutais avec Éric Walter qui est le secrétaire général de l'Hadopi, il y a quelques mois, et qui me disait que lui le DPI ça lui faisait peur. Donc, je pense que quand on arrive à un moment où l'instance qui est censée être l'instance de régulation des vilains pirates sur Internet me dit elle-même qu'elle a peur du DPI, je pense qu'il y a des questions à se poser.

M. Frédéric Martel, journaliste. (1 h 33 min 21 s). Oui rapidement je pense que le problème du DPI, la difficulté c'est qu'aujourd'hui c'est une quasiment norme, si vous voulez, qui êtes d'ailleurs une norme de fait. Il y a certain nombre de laboratoires mais surtout aussi des gens qui ont fait des développements, et des groupes à la fois de normalisation mais aussi d'intérêts multiples dont des très grandes sociétés qui poussent le dispositif.

74 Impact d'Internet sur l'économie française : http://www.economie.gouv.fr/files/rapport-mckinsey-company.pdf

Donc le problème du DPI, c'est sauf si on arrivait à avoir une gouvernance mondiale, qu'on peut toujours espérer pour demain, mais qui permette sur des technologies de ce type soit de les interdire soit de les contrôler, il est là. Donc le problème qui se pose il est moins dans les solutions techniques si vous voulez qui sont disponibles, qui seront toujours développées, y compris parfois par des structures relativement petites parce que c'est quand même relativement accessible comme type de technologie, la difficulté de fond c'est l'usage que l'on fait de cette technologie. Donc c'est pour ça que je pense, il ne faut pas se tromper de sujet, le DPI on ne peut pas le condamner...

M. Christian Paul, député. (1 h 34 min 20 s). Si vous permettez, et la nature du pays auquel on les vend…

M. Frédéric Martel, journaliste. (1 h 34 min 23 s). Mais là vous avez raison…

M. Christian Paul, député. (1 h 34 min 24 s). Parce que pour moi, excusez-moi de vous interrompre, mais il est pas périphérique de voir que le gouvernement français affiche d'un côté des principes qui sont encore là dans le rapport[75] du ministre de la défense au Parlement, c'est-à-dire se donne une sorte de limite morale et politique -pas seulement morale mais politique également- à l'exportation d'outils de guerre et de police -duale comme tout le monde l'a dit- qui mettent en cause directement les populations civiles, hein. Donc un propos officiel et de l'autre côté une pratique, donc, après on peut dire ce qu'on veut sur l'indispensabilité de ces technologies ou plutôt sur le fait qu'elles sont aujourd'hui, non pas simplement indispensables, mais elles sont dans le paysage technologique, elles ont été créées, elles existent. Bon, le fait qu'elles existent ne signifie pas qu'elles soient obligatoires ni forcément indispensables sauf pour des applications de gestion du trafic ou des choses comme ça. Donc on n'est pas devant un sujet mineur quand même hein ?

M. Frédéric Martel, journaliste. (1 h 35 min 23 s). Non ce n'est pas ce que j'ai dit, et je crois que sur ce point-là on va converger, on avait l'air d'être en opposition on va plutôt converger. Moi il me semble si vous voulez, que dans les remarques que j'ai fait, c'est de dire, attention de ne pas nous tromper en posant, j'allais dire de faux problèmes, en essayant de trouver de fausses solutions, par exemple dire « le DPI on peut s'en passer », ou des solutions de ce type. Je pense que ça renvoie difficilement aussi à simplement du juridique pur, puisqu'on a vu qu'on était multi-domaines c'est-à-dire qu'on n'était pas uniquement sur une législation d'un seul État, donc ça renvoie à des problèmes de gouvernance générale qui sont nécessaires, qu'il faut faire progresser sur ce point-là, mais on voit bien en même temps que l'outil juridique à ses limites, on l'a évoqué tout à l'heure et y compris sur le plan du droit pénal. Je pense qu'une bonne partie si vous voulez du dispositif vient à travers le rôle du politique ; donc là-dessus je vous rejoins sur le fait de pouvoir montrer à la fois les difficultés, pousser à des contrôles et le contrôle n'est pas forcément le contrôle d'une commission, parce qu'une commission après tout peut être aussi sous pression, mais c'est à travers le contrôle politique qu'assurent les instances comme l'assemblée, comme tout citoyen, comme la presse et les médias.

Par contre c'est vrai qu'on peut avoir des situations un peu délicates. Je pose par exemple une question, faut-il qu'à un moment un gouvernement -ou une instance peu importe- autorise ma foi, des outils de contrôle, qui à un moment peuvent être justifiés pour des problèmes de contrôle, je suis par exemple dans un État démocratique hein, je mets en place par exemple des outils de type contrôle, parce que là mon problème ne va pas être de courir après des opposants comme dans un régime totalitaire, mais va être principalement peut-être de lutter contre des déviances, comme un outil de police, contre des déviances qu'on avait indiquées, personne ne le conteste. [Commentaire inaudible en fond]

M. Christian Paul, député. (1 h 37 min 13 s). Donc c'est un débat qui est assez ancien maintenant, ça se fait dans le cas de procédure judiciaire, avec un emploi très strictement encadré, et là il y a pas eu ce soir me semble-t-il réellement débat sur ce point.

75 Rapport au Parlement sur les exportations d'armement de la France en 2010 : http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics//114000643/0000.pdf

M. Frédéric Martel, journaliste. (1 h 37 min 26 s). Nous sommes d'accord, mais on voit bien, c'est dès qu'on est au-delà du domaine national, on a une difficulté, et on voit bien aussi que, dès qu'il y a un changement de situation, et on peut espérer qu'on soit nous, en France où tout au moins en Europe, pas trop menacés sur le plan démocratique, encore que l'histoire a démontré que ce n'était jamais un combat gagné, donc on voit bien une situation, à un moment, par le bouleversement des autorités politiques, le même système qui était, si vous voulez, on va dire légitime dans son utilisation, devient à ce moment-là, ... donc on a un vrai problème de contrôle.

M. Christian Paul, député. (1 h 37 min 58 s). Donc on comprend bien ce que voulait dire Frédéric Martel, je crois qu'on a compris, simplement pardonnez-moi là aussi, sauf que dans le cas qui nous intéresse là, on n'est pas passé de la liberté et de la démocratie à la dictature, on était dans la dictature et on a vendu à ces pays dans des conditions effectivement infiniment mal contrôlées et encadrées…

M. Antoine Champagne, cofondateur Reflets.info. (1 h 38 min 17 s). Juste pour rebondir sur tout ça, c'est quand même assez simple à comprendre. Le marché du DPI, en gros, c'est quoi ? C'est la gestion plus ou moins des réseaux, alors parfois effectivement utile sur des réseaux 3G, des choses comme ça, ce sont des petits marchés, on parle de grande croissance etc. Mais ce sont de petits marchés. Amesys, juste pour finir sur les histoires de contrat en cours, est en train de répondre à Orange pour déployer du DPI en masse, on l'a écrit l'autre jour sur Reflets. Il y a ce marché-là, il y a le marché de l'écoute légale, en France par exemple pourquoi pas, personnellement je ne sais pas qui est le fournisseur de technologies, je crois que c'est Thales, hein c'est ça, qui installe la grosse plate-forme actuelle… [Commentaire inaudible en fond]

M. Jean-Marc Manach, journaliste. (1 h 39 min 09 s). Je crois que c'est Thales oui qui a remporté le marché…

M. Antoine Champagne, cofondateur Reflets.info. (1 h 39 min 11 s). Oui, Thales, Mais qui est derrière ? Parce que Thalès ce n'est pas un spécialiste de ces chose-là, donc y a surement un sous-traitant, et j'aimerais bien savoir qui c'est. [Commentaire inaudible en fond] Oui, bien sûr. Et l'autre marché qui lui, est probablement plus juteux, ce sont uniquement les dictatures et les états policiers, parce que c'est eux qui ont un intérêt à écouter de manière globale leur pays sans contrôle. [Commentaire inaudible en fond] Tout le monde… Bien sûr, mais si vous vendez…

M. Frédéric Martel, journaliste. (1 h 39 min 38 s). … Mais la croissance économique, ça passe aussi par ces outils là. Tout le monde a intérêt…

M. Antoine Champagne, cofondateur Reflets.info. (1 h 39 min 41 s). Mais vous allez vendre…

Intervenant non reconnu. (1 h 39 min 43 s). … C'est plus ou moins délicat mais…

M. Antoine Champagne, cofondateur Reflets.info. (1 h 39 min 44 s). La plate-forme qui a été vendue en Libye, allez-vous pouvoir la vendre et l'installer en France, pour pouvoir écouter l'ensemble des communications françaises ?

M. Jean-Marc Manach, journaliste. (1 h 39 min 51 s). Non ce n'est pas possible…

M. Antoine Champagne, cofondateur Reflets.info. (1 h 39 min 52 s). Non. Pourquoi ? Parce qu'il y a plusieurs fournisseurs d'accès et pour des raisons légales, il y un encadrement. Donc vous allez choisir un client qui est évident, qui est M. Kadhafi, qui est un dictateur connu, reconnu, terroriste, etc.

M. Jean-Marc Manach, journaliste. (1 h 40 min 05 s). Ce qui était très intéressant… [Commentaire inaudible en fond]

M. Antoine Champagne, cofondateur Reflets.info. (1 h 40 min 08 s). Ce sont ces marchés qui sont intéressants pour ces entreprises, mais ça reste, juste pour finir, des marchés qui sont petits. Si c'est des 20 25 millions d'euros, ce n'est pas énorme.

M. Jean-Marc Manach, journaliste. (1 h 40 min 25 s). Ce qui était très rigolo à Milipol c'est…

M. Christian Paul, député. (1 h 40 min 28 s). Pardon enfin, ce n'est pas totalement probant, parce que, on peut imaginer qu'aujourd'hui la quasi-totalité des pays du monde sont acheteur potentiellement, pour des raisons je l'espère différentes, de ces technologies-là, ça fait pas d'ailleurs, forcément des marchés en milliards d'euros ou de dollars, mais ça fait probablement un marché mondial. Ce qui explique d'ailleurs, la croissance des entreprises qu'on évoque-là. Ça explique aussi que c'est un sujet effectivement, où il y a des intérêts économiques évidemment en jeu, qui sont à l'échelle de la France sans doute pas totalement négligeables, ou en tout cas qui ne sont pas négligés, parce que si c'était un sujet totalement mineur, je pense qu'on aurait eu depuis longtemps une réponse du gouvernement aux questions qui ont été posées.

M. Antoine Champagne, cofondateur Reflets.info. (1 h 41 min 12 s). C'est pas mineur, ce n'est pas ce que je veux dire, quand on parle juste de croissance par exemple Qosmos on nous a parlé de cinq ou neuf mille pour-cent de croissance, il faut regarder d'où on part et à combien on arrive, il faut juste un peu relativiser un tout petit peu les choses.

M. Christian Paul, député. (1 h 41 min 30 s). Je vous propose un dernier tour de table ici.

M. Jean-Marc Manach, journaliste. (1 h 41 min 35 s). Ce que je voulais dire tout à l'heure, ouais ce qui était rigolo en un sens c'est qu'à Milipol, il y a un journaliste qui a demandé à un représentant d'Amesys, « est-ce que vous pouvez me faire démonstration de comment fonctionne Eagle ? ». La réponse du commercial ou du représentant Amesys est de dire, « ah non je ne peux pas le faire parce que c'est illégal en France ».

Pour revenir sur la question que vous avez posée tout à l'heure sur la prolifération, je vais prendre le cas de Qosmos. Qosmos donc, qui a été développée par une équipe du CNRS, qui est devenue une Start-up, donc. Le gouvernement, via le FSI, a investi dans Qosmos. Je n'ai pas la liste de tous les clients de Qosmos, mais raisonnablement vu ce que j'en sais aujourd'hui, une bonne partie des clients de Qosmos c'est pas des Kadhafi pour espionner des dissidents, ou voilà. Par contre ce qu'on sait, c'est que quand Amesys, enfin I2E à l'époque, vend Eagle, et c'est marqué commission R226 sur la plaquette d'Eagle, et c'est « *designé* », créé, pour Kadhafi d'ailleurs -parce que Amesys avait créé ça pour Kadhafi (enfin I2E)- comme un système d'interception globale des télécommunications à l'échelle d'une nation. Là on est bien un marchand d'armes qui vend. Donc la question pour moi, c'est pas tant de réguler la notion de DPI, que d'étendre le « R226 », et de faire rentrer le matériel, donc classifier « R226 », *atteinte à la vie privée*, le matériel d'interception des télécommunications à la liste du matériel de guerre, et faire de telle sorte que, on ne soit plus dans cette situation où on découvre à l'occasion du printemps arabe que les dictateurs étaient équipés par des entreprises occidentales, liées aux démocraties.

J'ai donné le nom des entreprises qui opérait en Tunisie d'après Bloomberg[76], donc c'était McAfee, entreprise américaine pour le filtrage Internet, Trovicor ex-Siemens-Nokia et Utimaco deux entreprises allemandes pour les interceptions téléphoniques, et pour ce qui est du DPI c'était ETI, qui est une entreprise britannique filiale de BAE-System. Donc à partir du moment où on sait que les principaux de ces marchands d'armes sont aux États-Unis, en Allemagne, en Grande-Bretagne, en France, en Italie, en Israël -et voilà, les principaux marchands d'armes- mettre en place un système de non-prolifération, qui permet -mais comme ça se passe pour le nucléaire, comme ça se passe pour les armes bactériologiques-chimiques - de vérifier qu'il n'y a pas de contrat qui permettrait à un dictateur d'acheter du matériel pour fabriquer des systèmes d'interception des communications et de surveillance massive de l'Internet. On arrive à le faire pour un certain nombre de

76 Post-Revolt Tunisia Can Alter E-Mail With `Big Brother' Software : http://www.bloomberg.com/news/2011-12-12/tunisia-after-revolt-can-alter-e-mails-with-big-brother-software.html

produits, pour ce qui relève du bactériologique, du chimique, et du nucléaire, je vois pas pourquoi si on arrive à le faire pour certains produits on ne pourrait pas à le faire pour d'autres. Ce n'est pas forcément très compliqué. En l'espèce, en attendant de trouver les ressorts techniques ou juridiques de ça, on sait très bien et c'est la vraie question qu'il faut poser maintenant, *est-ce que c'est normal qu'une démocratie aide une dictature à chasser des démocrates ?* Non. Et ça il va falloir trouver une solution politique à ça, parce que ce n'est pas normal… [Question inaudible en fond]

M. Olivier Laurelli, cofondateur Reflets.info. (1 h 44 min 16 s). Quel genre en fait de pays va écouter l'ensemble de sa population ? Est-ce que vous connaissez beaucoup de démocraties qui vont en plus vous l'avouer ? On va écouter l'ensemble de la population parce que vous êtes tous des terroristes, et des pédophiles -effectivement le pédophile est très en vogue également pour la vente de ce système...

M. Jean-Marc Manach, journaliste. (1 h 44 min 39 s). Je vais donner un exemple, le Mexique a acheté une solution russe, ce que j'ai découvert à Milipol, où ils enregistrent l'intégralité des télécommunications avec des systèmes de reconnaissance biométrique vocale, pour repérer les narcotrafiquants. Le Mexique n'est pas non plus une dictature, voilà donc, il y a au moins un pays qui a commencé à le faire à l'échelle téléphonique. [Question inaudible en fond]

Intervenant non reconnu. (1 h 45 min 01 s). Le Mexique est aussi client d'Amesys…

M. Olivier Laurelli, cofondateur Reflets.info. (1 h 45 min 11 s). Ecoutez, a priori je pense que je n'ai pas grand-chose à rajouter, si ce n'est qu'on va sûrement vous reparler d'autres petits pays assez sympathiques, dans lesquels la France exporte en plus de ses droits de l'homme de manière sporadique pas mal de DPI, dont le Kazakhstan, on reviendra sur le Maroc je présume également, eh bien on est pas au bout de nos surprises tout simplement, tu viens de parler du Mexique…

M. Jean-Marc Manach, journaliste. (1 h 45 min 36 s). Si je peux juste conclure, et pour répondre en partie à la question qui était posée tout à l'heure sur le fait de déchiffrer les communications, je pense que c'est très intéressant de voir comment au niveau de la directive européenne, l'anecdote que je racontais enfin c'est pas une anecdote, c'est ce qui s'est passé au Parlement européen, à savoir que sous la pression visiblement de la Grande-Bretagne et de l'Allemagne, les outils d'attaque informatique, de lutte informatique offensive, ont disparu du projet de réglementation. Et je pense que si on doit poser le débat politique, de savoir qu'est-ce que des entreprises dans une démocratie ont le droit de vendre à des pays qui ne sont pas démocratiques, et même au-delà des démocraties, qu'est-ce qu'on a le droit de vendre ou pas. Qu'est-ce qui est trop dangereux ? Et ben je pense qu'il ne faut pas seulement mettre les outils de surveillance informatique des télécommunications et d'interceptions, mais également les outils d'attaque, de lutte informatique offensive, pour reprendre le terme consacré, parce qu'on sait très bien que plus les gens vont être surveillés plus ils vont utiliser la crypto, ce qui s'est passé avec l'Hadopi. Plus les gens vont utiliser la crypto, plus on va utiliser des chevaux de Troie et des outils de lutte informatique offensive. Et que si on pose pas la question dès maintenant, comme Gmail, Facebook, Twitter, généralisent le fait de se connecter de façon chiffrée, mais avec les limites que ça a, le SSL, le SSH en ce moment, ou l'exemple des tours de Bluecoat en Syrie, pour éviter qu'on puisse se connecter de façon sécurisée à Facebook, je pense qu'il faut se poser la question de la lutte informatique offensive dès maintenant, parce que sinon, on va régler un problème qui était celui d'hier, et pas seulement celui de demain.

M. Jean-Marc Salmon, chercheur. (1 h 47 min 01 s). Oui écoutez, le débat est passionnant, alors je reste avec une idée extrêmement simple, parce que avec beaucoup d'éléments, il faut faire simple. Moi je pense qu'il faut mettre en avant la Syrie. Pourquoi la Syrie ? Ben parce qu'en ce moment les gens meurent en Syrie. Tous les jours des gens meurent en Syrie, il y a en ce moment une trentaine de blogueurs en Syrie qui sont en prison. Il y en a dont on est sans nouvelles depuis leurs arrestations. Alors la question des matériels qui permettent de contrôler les blogueurs et les internautes en Syrie, c'est quand même une question pour certaines personnes

qui est une question de vie ou de mort. Alors je pense que c'est là-dessus qu'il faut parler maintenant, c'est la première chose sur laquelle il faut parler, et il faut demander un moratoire immédiat, d'assistance technique, déguisée ou pas déguisée, par sous-traitance ou pas par sous-traitance, etc. en Syrie. C'est une procédure politique extrêmement simple, il suffit que le conseil européen à la liste des sanctions rajoute deux lignes. C'est quand même extrêmement simple. Il y a pas besoin de législation, de faire ceci, ou faire cela, il suffit que le conseil européen fasse ça. Et là c'est fini, AREA dénonce sont contrat demain matin, Qosmos dénonce son contrat demain matin, etc., en disant *c'est un cas de force majeure, vous avez vu, on nous a interdit*. Les Syriens, quand même, qui se battent depuis 9 mois et demi, à la différence des Tunisiens, où quand même le soulèvement s'est passé en un mois, ou les libyens où ça s'est passé en cinq mois ou six mois, et avec quand même, une aide militaire cachée mais importante de beaucoup de pays, les Syriens ils sont tous seuls. Et je pense que si le message arrivait à Alep, que quand même les histoires de contrôle d'Internet, ça suffit, et que oui, on fait quelque chose, ben je pense que les gens seraient contents pour Noël en Syrie, voilà ce que je pense. Il faut parler de choses simples à mon avis, dans ces affaires, à partir de là évidemment il faut poser la question, que ça ne se renouvelle pas, et donc d'un cadre législatif. Et le cadre législatif, on voit bien, et là je ne vais pas durer longtemps, les sociétés sont toutes américaines ou européennes. Si l'union européenne prend des positions, et prend des « *guidelines* », et prend des décisions, l'affaire est très avancée.

M. Jean-Marc Manach, journaliste. (1 h 49 min 37 s). Il semble que c'est le représentant français au conseil de sécurité de l'ONU qui a piqué un coup de gueule y a deux jours[77] en disant, c'est scandaleux, l'inaction des instances internationales par rapport à ce qui se passe en Syrie. Balayons devant notre porte, on sait qu'il y a une boîte française dont le matériel est utilisé aujourd'hui en Syrie, demandons ce qu'il en pense au représentant français au conseil de sécurité.

M. Jean-Marc Salmon, chercheur. (1 h 49 min 55 s). Moi je pense comme toi, c'est-à-dire que si l'affaire monte publiquement, ils ne peuvent pas tenir, ils sont obligés de céder, et Juppé, Ashton, et Clinton, etc., ils sont obligés de signer et de dire « oui, moratoire, Syrie ». Parce que c'est trop contradictoire.

M. Christian Paul, député. (1 h 50 min 17 s). Oui sur le dernier point qu'invoque Jean-Marc Salomon, je pense que c'est vrai, ce n'est pas seulement vrai tactiquement, mais je pense que c'est le bon combat maintenant. Vous avez passé beaucoup de temps sur la Libye, et c'était indispensable. Il faut bien sûr faire toute la lumière sur ce qui s'est passé en Libye, mais si on a la possibilité par exemple d'interpeller le gouvernement, que ce soit l'assemblée ou le Sénat dans les semaines qui viennent, je suis d'accord sur l'idée qu'il faut le faire avant tout sur la Syrie. D'abord parce qu'il y a une urgence politique et humaine évidente, mais aussi parce que c'est une façon de mettre en résonnance ce débat peut-être davantage, que sur le terrain libyen ou tunisien, qui, à tort sûrement, mais pourraient être jugé un peu trop historiques et un peu trop datés, même si je pense que c'est parce que vous avez réussi à mettre le projecteur très fortement sur la Libye, qu'on est conscient aujourd'hui que ces technologies sont en pleine prolifération, et qu'elles sont aussi en Syrie.

Alors peut-être deux trois mots pour conclure, pas pour synthétiser, mais peut-être pour répondre au fond à une question qui a été posé de plusieurs manières de ce côté-ci, c'est au fond est-ce qu'on est dans l'impuissance, ou est-ce qu'on peut faire quelque chose ? Est-ce que ça sert à quelque chose de se réunir là, et puis de mener des combats en apparence isolés. Bon, d'abord ça permet aussi quand même de constituer un peu plus de communautés autour de ces questions. Entre des « hacktivistes », des journalistes, des politiques, des informaticiens, citoyens etc., je crois que c'est important qu'il y ait des réseaux, peut-être plus nombreux encore, qui se mobilisent autour de ces questions. Et c'est l'effet d'amplification effectivement qu'on recherche. Et que -encore une fois- un certain nombre de médias ont commencé à capter, bon simplement aujourd'hui dans l'état où est le service public de l'audiovisuel, ils n'ont même pas les moyens d'aller mener des vraies enquêtes sur ces questions-là. Puisque nous avons un producteur de radio du service public dans la salle, peut être qu'il pourra aller lui aussi, lancer l'alerte avec nous.

77 Syrie : Paris dénonce le silence de l'ONU : http://www.lemonde.fr/proche-orient/article/2011/12/12/le-bilan-de-la-repression-en-syrie-s-eleve-a-5-000-morts-selon-l-onu_1617680_3218.html

Une commission d'enquête parlementaire ça ne règle pas tous les problèmes. Je réponds à votre question. Simplement, ça permet quand même de faire la lumière, ça permet de baliser complètement le terrain, parce que là on voit bien qu'on est dans la part d'ombre complète à la fois de l'Internet, du quinquennat qui s'achève, et également des ventes de technologies de police et de guerre. Donc une commission d'enquête parlementaire, c'est un gros coup de projecteur, ça permet non seulement d'identifier des responsabilités pour le passé, mais quand même de faire des propositions de modifications législatives, voilà c'est à ça que ça peut servir. De la même façon qu'une table ronde comme celle-là, si on en tire tous les leçons, les fruits, en tout cas, c'est ce que je m'efforcerai de faire avec ceux qui travaillent avec moi sur ces questions, c'est faire en sorte que, quand on travaille au changement des règles du jeu, que ce soit la législation française ou des règles européennes, on ne le fait pas non plus dans l'opacité. Quand on a fait des lois dans l'opacité, ça a donné Hadopi, par exemple, où effectivement il y a eu un simulacre de consultation mais il y a eu surtout beaucoup de choses qui se sont jouées dans le « *back office* » des palais de la république. Ce travail-là sert aussi à élaborer ensemble le changement des règles du jeu, ça se fait pas en trois jours, mais ça peut quand même se faire en quelques mois si on s'y prend bien. Et enfin pour redire en terminant, je crois qu'on n'est vraiment pas sur un sujet périphérique, puisqu'à un moment donné il y avait un peu cette interrogation, cette inquiétude.

Je crois qu'on est devant un double langage d'État total, d'un côté on célèbre les printemps démocratiques du monde arabe, et puis de l'autre côté on poursuit très loin, quasiment encore aujourd'hui, des ventes de technologie de surveillance et de répression. Il faut dire stop à ça. Si ce pays veut rester encore fidèle à son historique démocratique et au message des droits de l'homme, il doit le faire. Et d'ailleurs aujourd'hui, si on est un responsable politique français, on a aussi le choix entre encourager la vente de ces technologies, on n'a pas évoqué les problèmes de commission et de rétro-commissions qui entourent peut-être certaines de ces ventes-là. Ça faisait trop pour aujourd'hui, mais enfin, vu l'un des intermédiaires qui a été cité à un moment donné du débat, on peut quand même se demander, hein, c'est intéressant. Bon je pense qu'ici on est plutôt favorable à mettre à la disposition des cyberdissidents des kits qui leur permettent de mener leur combat. Voilà il y a peut-être là, deux façons de regarder ce que doit être le rôle et le message de la France à l'échelle internationale, et je ne vois pas pourquoi on laisserait à Hillary Clinton le monopole de la défense des cyberdissidents. Je pense que ça peut être aussi une position politique française très forte dans les mois qui viennent… S'en empare qui veut, mais enfin, j'ai aussi quelques idées sur la question.

Et puis après il y a vraiment un travail de fond, ça se fait toujours dans la durée, comment on change les règles de droit, on a vu ce soir qu'il y avait quand même, au plan français et européen de très grandes choses à faire, et que on avait besoin de sortir, encore une fois, des zones d'ombre dans lesquelles toutes ces questions ont été jusqu'à ces derniers mois, soigneusement camouflées.

Alors merci à vous, à vous, et puis voilà, comme on dit, on reste plus qu'en contact, et ceux qui veulent continuer à mener ensemble ces batailles sont les bienvenus, merci beaucoup.

***

[Fin de la Table ronde et de l'enregistrement sonore.]

Où en est-on aujourd'hui ?

Les lecteurs de *Reflets* ayant mis en forme ce document vous invitent à consulter tous les liens, notes et annexes référents insérés dans le document pour appuyer les propos des uns et des autres. En date de finalisation de ce document, le site *Arrêts sur Images* a réalisé une synthèse[78] chronologique des évènements, révélations et enquêtes associées à ce dossier et des implications d'entreprises et d'organismes institutionnels français ; *Owni* revient[79] sur l'action des Telecomix[80] à l'occasion des rencontres du *28e Chaos Computer Congress* (28C3)[81], les médias en ligne ou traditionnels continuent d'alerter et de sensibiliser de plus en plus bruyamment, comme *Arte*[82] ou encore *Forbes*[83] pour les derniers articles en date… Et puisque les révélations de *Reflets* sont « trop compliquées[84] » et que les médias et les citoyens ont du mal à (ou ne veulent pas) s'en emparer, le site a réalisé[85] un portail[86] dédié à la vulgarisation de toutes les formes de surveillances numériques. La technicité de ces technologies ne doit pas être une excuse pour ne pas s'en soucier.

Un jour certains devront rendre des comptes pour leur implication active ou leur complicité passive. Nul ne pourra prétendre qu'il ne savait pas. **Il s'agit aujourd'hui de questions de vie ou de mort pour des milliers de civils à travers le monde**, il s'agit demain de nos libertés numériques et de la neutralité du Net.

78 Avec Amesys, la France espionne au service de Kadhafi ? : http://www.arretsurimages.net/contenu.php?id=4575
79 Telecomix crée la mémoire vive des révolutions : http://owni.fr/2011/12/30/telecomix-cree-la-memoire-vive-des-revolutions/
80 Telecomix : http://telecomix.org/
81 28c3 Behind enemy lines : http://events.ccc.de/category/28c3/
82 La souris et le dictateur : http://www.arte.tv/fr/La-souris-et-le-dictateur/6299208.html
83 Tyrants and Technology: How Western Mercantilism Leads to Censorship and Disappearances : http://www.forbes.com/sites/thorhalvorssen/2011/12/29/tyrants-and-technology/
84 Reflets : c'est trop compliqué tes histoires… : http://reflets.info/reflets-cest-trop-complique-tes-histoires/
85 Surveillances : http://reflets.info/surveillances/
86 Surveillances : https://secure.reflets.info/

ANNEXE 1

Index croissant des questions de l'Assemblée Nationale posées au gouvernement restées sans réponse

Question N°**117381** du 06 septembre 2011 par Christian Paul (SRC)

http://www.nosdeputes.fr/question/QE/117381 http://questions.assemblee-nationale.fr/q13/13-117381QE.htm

M. Christian Paul interroge M. le ministre d'État, ministre des affaires étrangères et européennes, sur le rôle de l'État français dans la vente et l'emploi d'armes technologiques destinées à la surveillance de l'internet en Libye. Le droit à la connexion pour tous et les libertés numériques font aujourd'hui partie des principes que notre République doit défendre sans faiblir. Or les inquiétantes révélations d'observateurs nombreux reprises par les médias français ainsi que par le quotidien américain Wall street journal conduisent à penser que des technologies françaises destinées à la surveillance des communications numériques, appelées Deep Packet inspection (DPI), ont été vendues à la Libye au cours des dernières années. L'exportation de ces outils d'analyses des échanges numériques (messageries, réseaux sociaux...) commercialisées par les entreprises françaises doit à l'évidence être soumis au contrôle et à l'autorisation des autorités françaises, car ils sont assimilables à des armes technologiques. Il lui demande s'il a été conduit à autoriser la vente de telles technologies à ce pays, voire à d'autres qui auraient exprimé le souhait de les acquérir. Si ces technologies avaient été commercialisées sans l'aval officiel de l'État, quelles mesures le Gouvernement entend-il prendre pour qu'à l'avenir, elles soient soumises à cette procédure, et ainsi, ne puissent être vendues à des régimes autoritaires ? Il souhaite également savoir dans quelles conditions des services civils ou militaires français auraient été chargés, comme d'autres informations le laissent entendre, d'accompagner la livraison de ces outils, voire d'en former les utilisateurs.

Question N°**121846** du 15 novembre 2011 par Jean-Claude Sandrier (GDR)

http://www.nosdeputes.fr/question/QE/121846 http://questions.assemblee-nationale.fr/q13/13-121846QE.htm

M. Jean-Claude Sandrier attire l'attention de M. le ministre d'État, ministre des affaires étrangères et européennes, sur les exportations de matériel de communication de la société Amesys au profit du régime de Mouammar Kadhafi, livré en 2008. Il est problématique de voir que ce matériel - qui a servi à identifier des défenseurs des droits de l'Homme qui, pour certains ont été emprisonnés et torturés - est absent des listes de matériel sous contrôle de la commission interministérielle d'étude des exportations du matériel de guerre. En application des articles 4 et 5 de la convention de l'ONU contre la torture « tout État partie veille à ce que tous les actes de torture constituent des infractions au regard de son droit pénal. Il en est de même de la tentative de pratiquer la torture ou de tout acte commis par n'importe quelle personne qui constitue une complicité ou une participation à l'acte de torture ». Il incombe donc à la France en tant que pays signataire de cette convention de prendre les mesures nécessaires afin de respecter et faire respecter ses dispositions. Dans un moment crucial pour les négociations sur le traité sur le commerce des armes dans lesquels la France joue un rôle majeur, il est essentiel de prévenir de tels transferts qui participent à de graves violations des droits humains et qui contreviennent également au critère n° 2 de la position commune de l'Union européenne.

Question N°**121848** du 15 novembre 2011 par Philippe Vitel (UMP)

http://www.nosdeputes.fr/question/QE/121848 http://questions.assemblee-nationale.fr/q13/13-121848QE.htm

M. Philippe Vitel attire l'attention de M. le ministre d'État, ministre des affaires étrangères et européennes, sur les exportations de matériel de communication de la société Amesys au profit du régime de Mouammar Kadhafi, livré en 2008. Il est problématique de voir que ce matériel - qui a servi à identifier des défenseurs des

droits de l'Homme qui, pour certains, ont été emprisonnés et torturés - est absent des listes de matériel sous contrôle de la Commission interministérielle d'étude des exportations du matériel de guerre. En application des articles 4 et 5 de la convention de l'ONU contre la torture, « tout État partie veille à ce que tous les actes de torture constituent des infractions au regard de son droit pénal. Il en est de même de la tentative de pratiquer la torture ou de tout acte commis par n'importe quelle personne qui constitue une complicité ou une participation à l'acte de torture ». Il incombe donc à la France en tant que pays signataire de cette convention de prendre les mesures nécessaires afin de respecter et faire respecter ses dispositions. Dans un moment crucial pour les négociations sur le traité sur le commerce des armes dans lesquels la France joue un rôle majeur, il est essentiel de prévenir de tels transferts qui participent à de graves violations des droits humains et qui contreviennent également au critère 2 de la position commune de l'Union européenne.

Question N°**121850** du 15 novembre 2011 par Daniel Paul (GDR)

http://www.nosdeputes.fr/question/QE/121850 http://questions.assemblee-nationale.fr/q13/13-121850QE.htm

M. Daniel Paul attire l'attention de M. le ministre d'État, ministre des affaires étrangères et européennes, sur les exportations de matériel de communication de la société Amesys au profit du régime de Mouammar Kadhafi, livré en 2008. Ce matériel, qui a servi à identifier des défenseurs des droits de l'Homme, parmi lesquels certains ont été emprisonnés et torturés, est cependant absent des listes de matériel sous contrôle de la Commission interministérielle d'étude des exportations du matériel de guerre. En application des articles 4 et 5 de la convention de l'ONU contre la torture « tout État partie veille à ce que tous les actes de torture constituent des infractions au regard de son droit pénal. Il en est de même de la tentative de pratiquer la torture ou de tout acte commis par n'importe quelle personne qui constitue une complicité ou une participation à l'acte de torture ». Il incombe donc à la France, en tant que pays signataire de cette convention, de prendre les mesures nécessaires afin de respecter et faire respecter ses dispositions. Dans un moment crucial pour les négociations sur le traité sur le commerce des armes dans lesquels la France joue un rôle majeur, il est essentiel de prévenir de tels transferts qui participent à de graves violations des droits humains et qui contreviennent également au critère n° 2 de la position commune de l'Union européenne. Il demande quelles sont les intentions de la France à cet égard.

Question N°**121852** du 15 novembre 2011 par Rudy Salles (NC)

http://www.nosdeputes.fr/question/QE/121852 http://questions.assemblee-nationale.fr/q13/13-121852QE.htm

M. Rudy Salles attire l'attention de M. le ministre d'État, ministre des affaires étrangères et européennes, sur les exportations de matériel de communication de la société Amesys au profit du régime de Mouammar Kadhafi, livré en 2008. Il est problématique de voir que ce matériel, ayant servi à identifier des défenseurs des droits de l'Homme qui, pour certains, ont été emprisonnés et torturés, est absent des listes de matériel sous contrôle de la commission interministérielle d'étude des exportations du matériel de guerre. En application des articles 4 et 5 de la convention de l'ONU contre la torture, il incombe à la France en tant que pays signataire de cette convention de prendre les mesures nécessaires afin de respecter et faire respecter ses dispositions. Dans un moment crucial pour les négociations sur le traité sur le commerce des armes dans lesquels la France joue un rôle majeur, il est essentiel de prévenir de tels transferts qui participent à de graves violations des droits humains et qui contreviennent également au critère n° 2 de la position commune de l'Union européenne. Il souhaiterait donc connaître sa position sur cette question.

Question N°**122726** du 22 novembre 2011 par Christian Paul (SRC)

http://www.nosdeputes.fr/question/QE/122726 http://questions.assemblee-nationale.fr/q13/13-122726QE.htm

M. Christian Paul attire l'attention de M. le ministre d'État, ministre des affaires étrangères et européennes, sur le rôle de l'État français dans la vente et l'emploi d'armes technologiques destinées à la surveillance de l'internet en Libye. Le droit à la connexion pour tous et les libertés numériques font aujourd'hui partie des principes que notre République doit défendre sans faiblir. Or les inquiétantes révélations d'observateurs nombreux, reprises par les médias français ainsi que par le quotidien américain *Wall street journal* conduisent à penser que des technologies françaises destinées à la surveillance des communications numériques, appelées « *Deep Packet inspection* » (DPI), ont été vendues à la Libye, au cours des dernières années. L'exportation de ces outils d'analyses des échanges numériques (messageries, réseaux sociaux..) commercialisées par les entreprises françaises doit à l'évidence être soumis au contrôle et à l'autorisation des autorités françaises, car ils sont assimilables à des armes technologiques. Il lui demande donc s'il a été conduit à autoriser la vente de telles technologies à ce pays, voire à d'autres qui auraient exprimé le souhait de les acquérir. Si ces technologies avaient été commercialisées sans l'aval officiel de l'État, quelles mesures le Gouvernement entend-il prendre pour qu'à l'avenir, elles soient soumises à cette procédure, et ainsi, ne puissent être vendues à des régimes autoritaires ? Il souhaite également savoir dans quelles conditions des services civils ou militaires français auraient été chargés, comme d'autres informations le laissent entendre, d'accompagner la livraison de ces outils, voire d'en former les utilisateurs.

Question N°**123032** du 29 novembre 2011 par Jacqueline Fraysse (GDR)

http://www.nosdeputes.fr/question/QE/123032 http://questions.assemblee-nationale.fr/q13/13-123032QE.htm

Mme Jacqueline Fraysse interroge M. le ministre d'État, ministre des affaires étrangères et européennes, sur les exportations de matériel de communication de la société Amesys au profit du régime de Mouammar Kadhafi, livré en 2008. Il est problématique de voir que ce matériel - qui a servi à identifier des défenseurs des droits de l'Homme qui, pour certains, ont été emprisonnés et torturés - est absent des listes de matériel sous contrôle de la commission interministérielle d'étude des exportations du matériel de guerre. En application des articles 4 et 5 de la convention de l'ONU contre la torture, " tout État partie veille à ce que tous les actes de torture constituent des infractions au regard de son droit pénal. Il en est de même de la tentative de pratiquer la torture ou de tout acte commis par n'importe quelle personne qui constitue une complicité ou une participation à l'acte de torture ". Il incombe donc à la France en tant que pays signataire de cette convention de prendre les mesures nécessaires afin de respecter et faire respecter ses dispositions. Dans un moment crucial pour les négociations sur le traité sur le commerce des armes dans lesquels la France joue un rôle majeur, il est essentiel de prévenir de tels transferts qui participent à de graves violations des droits humains et qui contreviennent également au critère n° 2 de la position commune de l'Union européenne.

Question N°**123674** du 6 décembre 2011 par Hervé Féron (SRC)

http://www.nosdeputes.fr/question/QE/123674 http://questions.assemblee-nationale.fr/q13/13-123674QE.htm

M. Hervé Féron attire l'attention de M. le ministre d'État, ministre des affaires étrangères et européennes, sur le rôle de la France dans la vente et l'emploi d'armes technologiques destinées à la surveillance de l'internet et donc de la population en Libye. D'inquiétantes révélations, reprises par les médias français ainsi que par le grand quotidien américain The Wall street journal conduisent à penser que des technologies françaises destinées à la surveillance des communications numériques, appelées deep packet inspection (DPI), ont été vendues à la Libye du Colonel Kadhafi au cours des dernières années. L'exportation de ces outils d'analyses des échanges numériques commercialisées par des entreprises françaises devrait de toute évidence être soumis au contrôle et à l'autorisation des autorités françaises, car ils sont assimilables à des armes technologiques. Si ces

technologies avaient été commercialisées sans l'aval officiel de l'État, quelles mesures le Gouvernement entend-il prendre pour qu'à l'avenir, elles soient soumises à cette procédure, et ainsi, ne puissent être vendues à des régimes autoritaires. Il souhaite également savoir dans quelles conditions des services civils ou militaires français auraient été chargés, comme d'autres informations le laissent entendre, d'accompagner la livraison de ces outils, voire d'en former les utilisateurs.

Question N°**123675** du 6 décembre 2011 par Hervé Féron (SRC)

http://www.nosdeputes.fr/question/QE/123675 http://questions.assemblee-nationale.fr/q13/13-123675QE.htm

M. Hervé Féron attire l'attention de M. le ministre d'État, ministre des affaires étrangères et européennes, sur le rôle de la France dans la vente et l'emploi d'armes technologiques destinées à la surveillance de l'internet et donc de la population en Libye. D'inquiétantes révélations, reprises par les médias français ainsi que par le grand quotidien américain The Wall street journal conduisent à penser que des technologies françaises destinées à la surveillance des communications numériques, appelées Deep Packet inspection (DPI), ont été vendues à la Libye du Colonel Kadhafi au cours des dernières années. L'exportation de ces outils d'analyses des échanges numériques commercialisées par des entreprises françaises devrait de toute évidence être soumis au contrôle et à l'autorisation des autorités françaises, car ils sont assimilables à des armes technologiques. Il lui demande d'abord s'il confirme ces informations et si oui, il lui demande s'il a autorisé la vente de telles technologies à ce pays ou à d'autres États qui auraient exprimé le souhait de les acquérir. Si tel ne devait pas être le cas, il lui demande si, à sa connaissance, d'autres États ont bénéficié de ces technologies avant qu'il entre en fonction dans ce ministère.

Question N°**123956** du 13 décembre 2011 par Christian Eckert (SRC)

http://www.nosdeputes.fr/question/QE/123956 http://questions.assemblee-nationale.fr/q13/13-123956QE.htm

M. Christian Eckert attire l'attention de M. le ministre d'État, ministre des affaires étrangères et européennes, sur le rôle de la France dans la vente et l'emploi d'armes technologiques destinées à la surveillance de l'internet et donc de la population en Libye. D'inquiétantes révélations, reprises par les médias français ainsi que par le grand quotidien américain The Wall street journal conduisent à penser que des technologies françaises destinées à la surveillance des communications numériques, appelées deep packet inspection (DPI), ont été vendues à la Libye du colonel Kadhafi au cours des dernières années. L'exportation de ces outils d'analyse des échanges numériques commercialisés par des entreprises françaises devrait de toute évidence être soumis au contrôle et à l'autorisation des autorités françaises, car ils sont assimilables à des armes technologiques. Il lui demande d'abord s'il confirme ces informations et, si oui, il lui demande s'il a autorisé la vente de telles technologies à ce pays ou à d'autres États qui auraient exprimé le souhait de les acquérir. Si tel ne devait pas être le cas, il lui demande si, à sa connaissance, d'autres États ont bénéficié de ces technologies avant qu'il entre en fonction dans ce ministère.

ANNEXE 2

Index croissant des questions de l'Assemblée Nationale posées au gouvernement ayant obtenues une réponse

Question N°**118710** du 27 septembre 2011 Hervé Féron (SRC)

http://www.nosdeputes.fr/question/QE/118710 http://questions.assemblee-nationale.fr/q13/13-118710QE.htm

M. Hervé Féron attire l'attention de M. le ministre d'État, ministre des affaires étrangères et européennes, sur l'information selon laquelle Paris aurait livré un véhicule permettant au colonel Kadhafi de fuir la Libye. Selon les révélations d'un excellent journal d'investigation, une société française aurait fourni en 2008 au régime libyen, avec l'accord de l'Élysée, un véhicule 4×4 furtif ultrasécurisé pour assurer la protection des déplacements de son dirigeant, Mouammar Kadhafi, autrefois ami du président de la République. Ce 4×4 aurait été fabriqué par la société française Amesys (ex-I2E), filiale de Bull, et a été fourni à Tripoli par l'intermédiaire d'un citoyen Franco-libanais par ailleurs inculpé dans le cadre d'une affaire liée aux attentats de Karachi, au Pakistan. Il lui demande si cette information est exacte.

Réponse émise le 20 décembre 2011 : Le ministère des affaires étrangères et européennes n'a pas connaissance d'une livraison d'un véhicule 4x4 furtif ultrasécurisé à l'ancien régime libyen. Aucune autorisation d'exportation de matériel de guerre n'a été délivrée à cette fin.

Question orale au gouvernement du 20 décembre 2011 par Christian Paul (SRC)

http://www.nosdeputes.fr/seance/5747#table_17157 http://www.assemblee-nationale.fr/13/cri/2011-2012/20120090.asp#P297_40458

Monsieur le Premier ministre, il est désormais confirmé qu'au cours des dernières années, des entreprises françaises ont vendu à des dictatures des matériels de surveillance de l'Internet permettant d'intercepter le courrier électronique, de pister la consultation des sites et de connaître l'usage fait par chacun des réseaux sociaux. Ces armes électroniques sont à la fois des outils de guerre et des outils de police. Dans ces dictatures, avec l'aide de la France et le soutien de l'État, elles sont devenues des armes de basse police destinées à surveiller la population et à espionner l'opposition, les journalistes et les avocats. Il s'agit de l'un des plus scandaleux manquements aux valeurs démocratiques au cours des années récentes. Pour la Libye du colonel Kadhafi, ces faits sont prouvés. Une liste des opposants surveillés grâce à ce matériel français est publique. Le rôle de M. Takieddine est cité dans la négociation de ces contrats, et l'on sait quelles relations il a entretenues au sommet de l'État et de l'UMP. En Syrie, où le pouvoir torture et assassine, tout pousse à croire que ces technologies sont encore actives aujourd'hui. Monsieur le Premier ministre, vous devez rendre des comptes à la représentation nationale, mais aussi à l'opinion mondiale et aux militants des révolutions arabes. Dix questions parlementaires sont restées sans réponse de la part du Gouvernement, et une commission d'enquête est demandée en vain à l'Assemblée nationale. Pourquoi ce silence assourdissant ? Ces faits et cette omerta abîment l'honneur de la France qui aurait dû, au contraire, soutenir les cyberdissidents. Que savez-vous réellement de l'usage actuel ou passé de ces technologies de surveillance de l'Internet, en particulier en Syrie ? Quelles autorisations administratives ont été accordées ? À quel niveau le feu vert politique a-t-il été donné ? Êtes-vous prêts à décider, dès aujourd'hui, d'un moratoire sur ces exportations et, pour l'avenir, à encadrer strictement leurs ventes et leur usage, à des États étrangers, mais aussi... [Temps de parole écourté].

Réponse de M. Gérard Longuet, ministre de la défense et des anciens combattants : Monsieur le député, en qualité de ministre de la défense, je me sens l'obligation de m'efforcer de répondre à votre question puisque vous semblez viser des matériels de défense. La France est un pays parfaitement exemplaire pour ce qui concerne l'exportation de ces matériels. De majorité en majorité, nous avons construit un dispositif qui permet

de n'autoriser les exportations, qu'elles soient le fait de grandes entreprises ou de PME, que dans le cadre d'un contrôle extrêmement strict. Depuis 1939, l'affaire n'est pas nouvelle, de CIEMG en CIEMG – je parle des commissions interministérielles des exportations des matériels de guerre –, nous autorisons ces exportations et nous contrôlons l'usage final du matériel. Vous posez une question fondamentale car elle suppose l'existence d'un détournement d'emploi de tel ou tel matériel. En ce qui concerne les télécommunications, force est de reconnaître qu'à ce jour, aucune commission interministérielle des exportations des matériels de guerre n'a été sollicitée en la matière. S'il y a eu détournement de l'emploi de ces matériels, notre devoir est d'adapter l'administration des exportations des matériels de guerre. Mais pouvons nous imaginer à tout instant quels détournements peuvent avoir lieu ? Vous nous reprocherez bientôt de ne pas contrôler les exportations alimentaires ou celles de biens de d'équipements – pour les vêtements des troupes, par exemple. Ce n'est simplement pas possible. Dans le cas particulier, je tiens à la transparence absolue : jamais la commission interministérielle n'a été sollicitée.

Question orale au gouvernement du 20 décembre 2011 par Daniel Goldberg (SRC)

http://www.nosdeputes.fr/seance/5747#table_17161 http://www.assemblee-nationale.fr/13/cri/2011-2012/20120090.asp#P370_58938

Monsieur le Premier ministre, le 9 août dernier, j'interrogeais le Gouvernement au sujet du versement supposé par la société i2e, devenue Amesys, filiale du groupe Bull, de commissions d'un montant de plusieurs millions d'euros à un ou plusieurs intermédiaires ayant favorisé la conclusion, en avril 2007, d'un contrat de technologies militaires à la Libye. Je demandais quelles poursuites avaient été engagées à l'encontre des sociétés et des personnes impliquées pour des faits proscrits par la loi depuis septembre 2000. Je n'ai obtenu aucune réponse. Le 27 septembre, je questionnais ici même M. le ministre de l'intérieur sur ses liens supposés, entre 2004 et 2009, avec le régime du colonel Kadhafi, sur l'objet des visites qu'il aurait effectuées à Tripoli à l'automne 2005, précédant de peu celles de Nicolas Sarkozy, puis de Brice Hortefeux, des visites préparées par l'intermédiaire Ziad Takieddine. Je n'ai obtenu aucune réponse. Depuis, plusieurs révélations tendent à démontrer que la vérité n'a pas été entièrement dévoilée. Le fait que le contrat signé en avril 2007, en pleine campagne présidentielle, avait reçu le plein soutien du ministre de l'intérieur de l'époque, Nicolas Sarkozy, n'y serait pas étranger. Aujourd'hui, pouvez-vous nous dire précisément comment votre gouvernement est impliqué dans ce dossier ? Pouvez-vous nous dire précisément quelles ont été vos relations avec l'ancien régime libyen, notamment avec Abdallah Senoussi, alors chef des services secrets libyens et condamné en 1999 pour sa responsabilité dans l'attentat du DC10 d'UTA, aujourd'hui arrêté et poursuivi par la Cour pénale internationale ? Avez-vous autorisé la vente en 2009 par i2e-Amesys d'un système de filtrage de l'Internet libyen – évoqué il y a quelques instants par Christian Paul –, système qui a permis d'espionner des opposants libyens dans le pays et à l'étranger ? La représentation nationale doit être informée au sujet de ces faits ! En somme, monsieur le ministre, étiez-vous au courant de la réalité de ces transactions, ce qui serait déjà grave, ou bien en étiez-vous les décideurs ?

Réponse de M. Claude Guéant, ministre de l'intérieur, de l'outre-mer, des collectivités territoriales et de l'immigration : Monsieur le député, j'ai déjà eu l'occasion de dire dans cette enceinte que, pour le bien de notre démocratie, il serait temps de mettre fin aux insinuations, aux amalgames, aux approximations et aux accusations sans fondement ! Aujourd'hui, je vous dis très clairement, en prenant mes responsabilités, que jamais le ministre de l'intérieur ni son entourage ne se sont occupés d'une telle transaction !